

# Separation of Reliability and Secrecy in Rate-Limited Secret Key-Distillation

Rémi A. Chou, *Student Member, IEEE* and Matthieu R. Bloch, *Member, IEEE*

## Abstract

For a discrete or a continuous source model, we study the problem of key distillation with one round rate-limited public communication between two legitimate users. Although, we do not derive new bounds on the wiretap secret-key (WSK) capacity for the discrete source model, we study an alternative achievability scheme that may be useful for practical application such as [quantum key distribution \(QKD\)](#) or physical-layer security, and that conveniently extends known bounds to the case of a continuous source model. Specifically, we consider a sequential key-distillation strategy, that implements a rate-limited reconciliation step to handle reliability, followed by a privacy amplification step performed with extractors to handle secrecy. We prove that such a sequential strategy leads to an optimal key-distillation (under the assumption of degraded sources in the case of two-way communication). Furthermore, we study under which conditions secrecy and reliability can be treated as independent problems. Finally, in the case of one-way rate-limited public communication, we illustrate our results for a binary and a Gaussian degraded source model.

## Index Terms

Wiretap secret-key capacity, sequential key-distillation, reconciliation, privacy amplification

## I. INTRODUCTION

Information-theoretic secret-key agreement protocols [1], [2] draw their strength from a security relying on information-theoretic metrics rather than on complexity theory, thereby avoiding the assumption of limited computational power for the eavesdropper. In such protocols, two legitimate users (Alice and

R. A. Chou and M. R. Bloch are with the School of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, GA 30332-0250 and GT-CNRS UMI 2958, 2 rue Marconi, 57070 Metz, France.

E-mail : remi.chou@gatech.edu; matthieu.bloch@ece.gatech.edu

Bob) and an eavesdropper (Eve) observe the realizations of correlated [random variables \(RVs\)](#), discrete or continuous. The legitimate users, who can exchange messages over a public channel, aim at extracting a common secret key from their observations. The rules by which the legitimate users compute the messages they exchange over the public channel and agree on a key define a key-distillation strategy. The maximum number of secret-key bits per observed realization of the [RVs](#) is called the wiretap secret-key (WSK) capacity [2], [3].

Closed-form expressions and bounds for the WSK capacity have been established for a large variety of models [1], [2], [3]. However, usual achievability proofs rely on a random binning argument and thus, do not always provide direct insight into the design of practical key-distillation strategies. Moreover, such proofs handle reliability (the legitimate users must share the same key) and secrecy (the key must be unknown to the eavesdropper) jointly, which creates a complex dependence between the public messages exchanged and the secret key constructed, and might limit the flexibility of the scheme.

For practical key-distillation, as in [QKD](#) [4], [5] or physical-layer security for wireless channels [6], a sequential key-distillation strategy is often used. Such a strategy consists of two steps that handle reliability and secrecy successively, instead of jointly. A reconciliation step [7] is first performed, during which Alice and Bob communicate over the public channel to agree on a common bit sequence, that might not be totally hidden from Eve. Then, a privacy amplification step [8], [9] is performed, during which Alice and Bob apply a deterministic function to their shared sequence to generate their common secret key, this time completely unknown from Eve.<sup>1</sup>

The main benefit of sequential key-distillation strategies is to separate how one deals with reliability and secrecy,<sup>2</sup> and thus to provide a perhaps more practical key-distillation design. Indeed, reconciliation can be efficiently implemented with LDPC codes [11], [12] and privacy amplification can be performed with hash functions or with extractors [8], [9]. While sequential key-distillation is studied in [9], [13], in the case of a public channel of unlimited capacity, we focus here on sequential key-distillation with

<sup>1</sup>As remarked in [10], when the eavesdropper has access to the messages publicly exchanged but not to a RV correlated to the legitimate users' ones, a close relation exists between the secret-key capacity and a source coding problem free from any secrecy constraint. The principle of sequential key-distillation strategies goes further, since it explicitly breaks down the protocol into two parts, one of which being free from any secrecy constraint. We show that this principle is optimal and applicable even if the eavesdropper has a RV correlated to the legitimate users' ones, i.e for the WSK capacity.

<sup>2</sup>We mean that the key-distillation can be performed by the succession of two protocols, one, free from any secrecy constraint, dealing with reliability, and the other dealing with secrecy. A stronger result would be that optimizing both protocols independently leads to the best possible key-distillation strategy. In Sections [IV-C](#) and [V](#), we prove that this stronger result holds in some cases (see Section [IV-C](#) for further clarifications).

rate-limited public communication to account for realistic constraints (real equipment may have limited bandwidth resources, such as in wireless sensor networks). Note that the achievability scheme of [14, Theorem 4.1], which only holds for Gaussians sources and when there is no side information at the eavesdropper, is very close to the sequential approach that we study, even though their model is different in that it deals with a quantized source and unrestricted public communication. Although, we do not improve WSK capacity bounds for the discrete source model, we provide an achievability scheme that might be easier to translate into practical designs. The main contributions of this work are:

- an alternative achievability scheme that separates reliability and secrecy by means of a reconciliation protocol and a privacy amplification step performed with extractors, which achieves
  - (i) the best known bound of the two-way one round rate-limited WSK capacity in the case of degraded sources;
  - (ii) the one-way rate-limited WSK capacity (it extends [15], in which degraded sources are assumed);
  - (iii) the two-way one round rate-limited SK capacity (no side information at the eavesdropper);

These results extend the bounds for a discrete source model in [3], to the case of a continuous source model (the case of the one-way rate-limited WSK capacity is treated in [16], but only for degraded sources);

- the proof that optimizing reconciliation and privacy amplification independently leads to the best possible key-distillation strategy for special cases, which is of prior importance to obtain a flexible coding scheme;
- the characterization of the rate-limited reconciliation capacity, which corresponds to the best trade-off between the length of the sequence shared by Alice and Bob after reconciliation and the quantity of information publicly exchanged;
- the illustration of the results for binary and Gaussian degraded sources, for which reconciliation and privacy amplification can be designed independently in the case of a one-way rate-limited public communication. This includes the determination of a closed-form expression of the WSK capacity for binary symmetric sources.

The remainder of the paper is organized as follows. In Section III, we formally introduce the problem studied in the paper. In Section IV, we characterize the one round rate-limited reconciliation capacity, and we prove that the sequential application of reconciliation and privacy amplification with extractors is an optimal key-distillation strategy. We also provide scenarios for which these two phases can be designed independently of each other. Finally, in Section V, we illustrate our results in the cases of binary and

Gaussian degraded sources for a one-way rate-limited communication. All proofs are gathered in the appendices to streamline presentation.

## II. NOTATION

Consider  $p, q \in \mathbb{R}$ . We define the following associative and commutative operation  $p \star q \triangleq p(1 - q) + (1 - p)q$ ; observe that  $[0, 1]$  is closed with respect to  $\star$ . We define the integer interval  $\llbracket p, q \rrbracket$ , as the set of integers between  $\lfloor p \rfloor$  and  $\lceil q \rceil$ . We define  $[p]^+$  as  $\max(0, p)$ . Finally, we note  $H_b(\cdot)$  the binary entropy, and  $(\mathcal{B}_c(K), \|\cdot\|_\infty)$  the set of  $K$ -bounded continuous function, where  $K \in \mathbb{R}$ .

## III. PROBLEM STATEMENT

As illustrated in Figure 1, a source model for secret-key agreement represents a situation in which two legitimate users, Alice and Bob, and one eavesdropper, Eve, observe the realizations of a memoryless source (MS)  $(\mathcal{X}\mathcal{Y}\mathcal{Z}, p_{XYZ})$ , that can be either discrete (DMS) or continuous (CMS). The three components  $X$ ,  $Y$  and  $Z$ , are observed by Alice, Bob, and Eve, respectively. The MS is assumed to be outside the control of all parties, but its statistics are known. Alice and Bob's objective is to process their observations and agree on a key  $K$ , about which Eve should have no information. We assume a two-way one-round communication between Alice and Bob, that is, we suppose that Alice first sends a message to Bob, and that in return Bob sends a message to Alice.<sup>3</sup> We also assume that the messages are exchanged over an authenticated noiseless public channel with limited rate; in others words, Eve has total access to Alice and Bob's messages, but cannot tamper with the messages over the channel. We now formally define a key-distillation strategy.

**Definition 1.** A  $(2^{nR}, n, R_1, R_2)$  key-distillation strategy  $\mathcal{S}_n$  for a source model with MS  $(\mathcal{X}\mathcal{Y}\mathcal{Z}, p_{XYZ})$  consists of

- a key alphabet  $\mathcal{K} = \llbracket 1, 2^{nR} \rrbracket$ ;
- two alphabets  $\mathcal{A}, \mathcal{B}$  respectively used by Alice and Bob to communicate over the public channel;
- two encoding functions  $f_0 : \mathcal{X}^n \rightarrow \mathcal{A}$ ,  $g_0 : \mathcal{Y}^n \times \mathcal{A} \rightarrow \mathcal{B}$ ;
- two functions  $\kappa_a : \mathcal{X}^n \times \mathcal{B} \rightarrow \mathcal{K}$ ,  $\kappa_b : \mathcal{Y}^n \times \mathcal{A} \rightarrow \mathcal{K}$ ;

and operates as follows

- Alice observes  $n$  realizations of the source  $X^n$  while Bob observes  $Y^n$ ;

<sup>3</sup>One could also suppose that Bob is the one who sends messages, in which case one only needs to exchange the role of  $X$  and  $Y$  in the following.

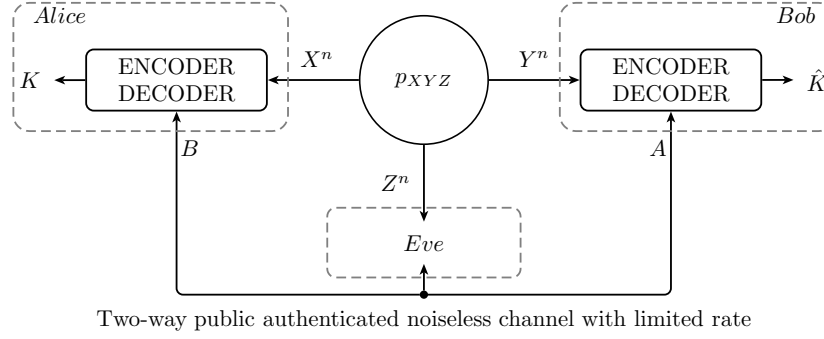


Fig. 1. Source model for secret-key agreement.

- Alice transmits  $A = f_0(X^n)$  subject to  $H(A) \leq nR_1$ ;
- Bob transmits  $B = g_0(Y^n, A)$  subject to  $H(B) \leq nR_2$ ;
- Alice computes  $k = \kappa_a(X^n, B)$  while Bob computes  $\hat{k} = \kappa_b(Y^n, A)$ .

The performance of a  $(2^{nR}, n, R_1, R_2)$  key-distillation strategy  $\mathcal{S}_n$  is measured in terms of the average probability of error between the key  $k$  generated by Alice and the key  $\hat{k}$  generated by Bob  $\mathbf{P}_e(\mathcal{S}_n) \triangleq \mathbb{P}[K \neq \hat{K} | \mathcal{S}_n]$ , in terms of the information leakage to the eavesdropper  $\mathbf{L}(\mathcal{S}_n) \triangleq I(K; Z^n | AB | \mathcal{S}_n)$ , and in terms of the uniformity of the key  $\mathbf{U}(\mathcal{S}_n) \triangleq \log[2^{nR}] - H(K | \mathcal{S}_n)$ .

**Definition 2.** A WSK rate  $R$  is achievable for a source model if there exists a sequence of  $(2^{nR}, n, R_1, R_2)$  key-distillation strategies  $\{\mathcal{S}_n\}_{n \geq 1}$  such that

$$\lim_{n \rightarrow \infty} \mathbf{P}_e(\mathcal{S}_n) = 0 \quad (\text{reliability}),$$

$$\lim_{n \rightarrow \infty} \mathbf{L}(\mathcal{S}_n) = 0 \quad (\text{strong secrecy}),$$

$$\lim_{n \rightarrow \infty} \mathbf{U}(\mathcal{S}_n) = 0 \quad (\text{strong uniformity}).$$

Moreover, the WSK capacity of a source model with MS  $(\mathcal{XYZ}, p_{XYZ})$  is the supremum of achievable WSK rates.

In the following, we also consider situations in which the eavesdropper has access to the public messages exchanged by Alice and Bob, but has no side information  $Z^n$ . In such cases, the WSK capacity is simply called the **secret-key (SK)** capacity and is denoted by  $C_{\text{SK}}$ .

For convenience, we recall here known results regarding the model.

**Theorem 1** ([3] Theorem 5, Theorem 6). *Let  $(\mathcal{XYZ}, p_{XYZ})$  be a DMS.*

(a) For  $R_1, R_2 \in \mathbb{R}^+$ , the two-way one-round WSK capacity satisfies

$$C_{\text{WSK}}(R_1, R_2) \geq R_{\text{WSK}}(R_1, R_2),$$

where  $R_{\text{WSK}}(R_1, R_2) = \max_{U,V} ([I(Y;U) - I(Z;U)]^+ + [I(X;V|U) - I(Z;V|U)]^+)$  subject to

$$R_1 \geq I(X;U|Y), \quad (1)$$

$$R_2 \geq I(Y;UV|X), \quad (2)$$

$$U \rightarrow X \rightarrow YZ \text{ and } V \rightarrow YU \rightarrow XZ,$$

$$|\mathcal{U}| \leq |\mathcal{X}|+2, |\mathcal{V}| \leq |\mathcal{Y}|. \quad (3)$$

(b) For  $R_1 \in \mathbb{R}^+$ , the one-way WSK capacity is

$$C_{\text{WSK}}(R_1, 0) = \max_{U,V} (I(Y;U|V) - I(Z;U|V)) \text{ subject to}$$

$$R_1 \geq I(X;U|Y),$$

$$V \rightarrow U \rightarrow X \rightarrow YZ,$$

$$|\mathcal{U}| \leq |\mathcal{X}|+1. \quad (4)$$

**Corollary 2** ([3] Theorem 2, Theorem 4). *Let  $(\mathcal{X}\mathcal{Y}, p_{XY})$  be a DMS.*

(a) For  $R_1, R_2 \in \mathbb{R}^+$ , the two-way SK capacity is

$$C_{\text{SK}}(R_1, R_2) = \max_{U,V} (I(Y;U) + I(X;V|U)) \text{ subject to}$$

$$U \rightarrow X \rightarrow Y, \quad (5)$$

$$V \rightarrow YU \rightarrow X, \quad (6)$$

rate constraints (1), (2), and range constraints (3).

(b) For  $R_1 \in \mathbb{R}^+$ , the one-way SK capacity is

$$C_{\text{SK}}(R_1, 0) = \max_U (I(Y;U)) \text{ subject to}$$

rate constraint (1), Markov condition (5), and range constraint (4).

For a DMS, in the absence of rate constraint between Alice and Bob, i.e.  $R_1 = +\infty$ , [13, Theorem 4.7] (see also [9]) states that we can handle reliability and secrecy successively to achieve the WSK capacity  $C_{\text{WSK}}(R_1, 0)$ , by means of a reconciliation step that deals with reliability, and a privacy amplification

step that deals with secrecy. In the next sections, we extend these results for a rate-limited communication between Alice and Bob, i.e.  $R_1, R_2$  finite, and in addition, we study under which conditions secrecy and reliability can be treated as independent problems. Specifically, we study the achievability of  $R_{\text{WSK}}(R_1, R_2)$ ,  $C_{\text{WSK}}(R_1, 0)$  (Theorem 1) and  $C_{\text{SK}}(R_1, R_2)$  (Theorem 2) with a sequential key-distillation strategy consisting of a two-way one round reconciliation protocol and a privacy amplification with extractors.

#### IV. SEQUENTIAL KEY-DISTILLATION STRATEGY

In the following, we use the term sequential key-distillation strategy, for a key-distillation strategy consisting of the succession of a reconciliation protocol and a privacy amplification with extractors.

##### A. Reconciliation

During the reconciliation phase, Alice and Bob send messages to each other over an authenticated public channel with limited rate. Alice and Bob then process their observations to agree on a common bit sequence  $S$ . At this stage the sequence is not subject to any secrecy constraint. Formally, a two-way one round rate-limited reconciliation protocol is defined as follows.

**Definition 3.** Let  $R_1, R_2 \in \mathbb{R}^+$ . A rate-limited reconciliation protocol  $\mathcal{R}_n(R_1, R_2)$ , noted  $\mathcal{R}_n$  for convenience, for a source model with MS  $(\mathcal{XY}, p_{XY})$  consists of

- an alphabet  $\mathcal{S} = \llbracket 1, M \rrbracket$ ;
- two alphabets  $\mathcal{A}, \mathcal{B}$  respectively used by Alice and Bob to communicate over the public channel;
- two encoding functions  $f : \mathcal{X}^n \rightarrow \mathcal{A}, g : \mathcal{Y}^n \times \mathcal{A} \rightarrow \mathcal{B}$ ;
- two functions  $\eta_a : \mathcal{X}^n \times \mathcal{B} \rightarrow \mathcal{S}, \eta_b : \mathcal{Y}^n \times \mathcal{A} \rightarrow \mathcal{S}$ ;

and operates as follows

- Alice observes  $n$  realizations of the source  $X^n$  while Bob observes  $Y^n$ ;
- Alice transmits  $A = f(X^n)$  subject to  $H(A) \leq nR_1$ ;
- Bob transmits  $B = g(Y^n, A)$  subject to  $H(B) \leq nR_2$ ;
- Alice computes  $S = \eta_a(X^n, B)$  while Bob computes  $\hat{S} = \eta_b(Y^n, A)$ .

The reliability performance of a reconciliation protocol is measured in terms of the average probability of error  $\mathbf{P}_e(\mathcal{R}_n) \triangleq \mathbb{P}[S \neq \hat{S} | \mathcal{R}_n]$ . In addition, since the reconciliation protocol, which generates the common sequence  $S$ , is followed by the privacy amplification step to generate a secret-key, it is desirable

to leak as little information as possible over the public channel. As in [13] we define the reconciliation rate of a reconciliation protocol as  $\mathbf{R}(\mathcal{R}_n) \triangleq \frac{1}{n} [H(S|\mathcal{R}_n) - H(AB|\mathcal{R}_n)]$ .

**Definition 4.** For a given  $(R_1, R_2)$ , a reconciliation rate  $R$  is achievable, if there exists a sequence of rate-limited reconciliation protocols  $\{\mathcal{R}_n\}_{n \geq 1}$  such that

$$\lim_{n \rightarrow \infty} \mathbf{P}_e(\mathcal{R}_n) = 0 \text{ and } \lim_{n \rightarrow \infty} \mathbf{R}(\mathcal{R}_n) \geq R.$$

Moreover, the two-way one round rate-limited reconciliation capacity  $C_{\text{rec}}(R_1, R_2)$  of a MS  $(\mathcal{X}\mathcal{Y}, p_{XY})$  is the supremum of achievable reconciliation rates.

The reconciliation capacity characterizes the best trade-off between the length of the sequence shared by Alice and Bob after reconciliation and the quantity of information publicly exchanged. We formally prove in Section IV and Section V that in some cases, optimizing reconciliation and privacy amplification independently, which implies achieving the reconciliation capacity, leads to the best possible sequential key-distillation strategy.

**Proposition 1.** Let  $(\mathcal{X}\mathcal{Y}, p_{XY})$  be a MS.

(a) For  $R_1, R_2 \in \mathbb{R}^+$ , the rate-limited reconciliation capacity  $C_{\text{rec}}(R_1, R_2)$  is

$$C_{\text{rec}}(R_1, R_2) = C_{\text{SK}}(R_1, R_2).$$

(b) Assume  $R_1 \in \mathbb{R}^+$  and  $R_2 = 0$ . For a DMS, we tighten the rate constraint (1) and the range constraint (4) as follows

$$C_{\text{rec}}(R_1, 0) = C_{\text{SK}}(R_1, 0) = \max_U I(Y; U) \text{ subject to}$$

$$R_1 = I(X; U|Y), \tag{7}$$

$$U \rightarrow X \rightarrow Y,$$

$$|\mathcal{U}| \leq |\mathcal{X}|.$$

For a CMS, (7) also holds, if the pdf  $f_{U|X}$  exists and is in  $\mathcal{B}_c(K)$ , for some  $K \in \mathbb{R}$ .

*Proof:* See Appendix A. ■

**Remark 1.** Let  $R_2 \in \mathbb{R}^+$ ,  $R_1 \in [H(X|Y), +\infty[$ . For a DMS,  $C_{\text{rec}}(R_1, R_2) = I(X; Y)$ .

**Remark 2.** In Proposition 1, the equality in the rate constraint (7) relies on an argument applicable to various convex maximization problems: the maximum principle (see Appendix A-A). This argument is



also used in Proposition 2. Note that the refinement offered by these equalities is critical to tighten the range constraints on  $\mathcal{U}$  in Propositions 1, 2, as well as to determine the WSK capacity for binary sources in Section V-A.

### B. Privacy amplification

During the privacy amplification phase, Alice and Bob generate their secret key by applying a deterministic function, on which they publicly agreed ahead of time, to their common sequence  $S$  obtained after reconciliation. This phase is performed with extractors [17], which are functions that take as input a sequence of  $n$  arbitrarily distributed bits and output a sequence of  $k$  nearly uniformly distributed bits, using another input of  $d$  truly uniformly distributed bits. The following theorem provides a lower bound on the size of the key, on which the legitimate users agree.

**Theorem 3** ([9], [13]). *Let  $S \in \{0, 1\}^n$  be the RV that represents the common sequence shared by Alice and Bob, and let  $E$  be the RV that represents the total knowledge about  $S$  available to Eve. Let  $e$  be a particular realization of  $E$ .*

*If Alice and Bob know that  $H_\infty(S|E = e) \geq \gamma n$ , for some  $\gamma \in ]0, 1[$ , then there exists an extractor  $g : \{0, 1\}^n \times \{0, 1\}^d \rightarrow \{0, 1\}^k$  with  $d \leq n\delta(n)$  and  $k \geq n(\gamma - \delta(n))$ . Moreover, if  $U_d$  is a RV uniformly distributed on  $\{0, 1\}^d$  and Alice and Bob choose  $K = g(S, U_d)$  as their secret key, then*

$$H(K|U_d, E = e) \geq k - \delta^*(n), \text{ with } \delta^*(n) = 2^{-\sqrt{n}/\log n} (k + \sqrt{n}/\log n).$$

Note that, the size  $d$  of the uniformly distributed input sequence is negligible, compared to  $n$ , so that the effect on the rate of public communication is negligible. Moreover, extractors that extract almost the entire min-entropy of the input  $S$  and require comparatively negligible amount of uniform randomness can be efficiently constructed [17].

**Remark 3.** *Privacy amplification can also be performed with hash functions, in which case the counterpart of Theorem 3 is found in [8]. However, the use of hash functions inflicts a penalty, since this requires more random bits than extractors. In fact, hash functions must be chosen at random in universal families, which requires on the order of  $n$  random bits, and translates into a communication rate loss of 1 bit, (see [8], [13] for further details).*

### C. Sequential key-distillation strategy

In this section, we prove our main result, namely, that the successive combination of reconciliation and privacy amplification achieves the best known rates.

**Theorem 4.** Let  $(\mathcal{X}\mathcal{Y}\mathcal{Z}, p_{XYZ})$  be a MS such that  $X \rightarrow Y \rightarrow Z$ . For  $R_1, R_2 \in \mathbb{R}^+$ , all WSK rates  $R$  that satisfy

$$R < R_{\text{WSK}}(R_1, R_2)$$

are achievable with sequential key-distillation strategies.

*Proof:* See Appendix B-A. ■

**Remark 4.** Note that we assume  $X \rightarrow Y \rightarrow Z$ . Common examples for which this hypothesis is valid, are sources generated over the degraded broadcast channel, or over channels such that  $p_{XZ|Y} = p_{X|Y}p_{Z|Y}$ , as in a wireless context for instance. For two-way communication, the necessity of this hypothesis might be an inherent weakness of a scheme that consists of a successive design of reconciliation and privacy amplification, rather than a joint design as in [3] (see the proof for more details). Observe, however, that for a one-way public communication (Theorem 5), this assumption is not required.

**Theorem 5.** Let  $(\mathcal{X}\mathcal{Y}\mathcal{Z}, p_{XYZ})$  be a MS. For  $R_1 \in \mathbb{R}^+$ , all WSK rates  $R$  that satisfy

$$R < C_{\text{WSK}}(R_1, 0)$$

are achievable with sequential key-distillation strategies.

*Proof:* See Appendix B-B. ■

**Theorem 6.** Let  $(\mathcal{X}\mathcal{Y}, p_{XY})$  be a MS.

(a) For  $R_1, R_2 \in \mathbb{R}^+$ , all SK rates  $R$  that satisfy

$$R < C_{\text{SK}}(R_1, R_2)$$

are achievable with sequential key-distillation strategies.

(b) Moreover, reconciliation and privacy amplification can be designed independently.

*Proof:* See Appendix B-C. ■

Theorem 5 and Theorem 4 state that a sequential key-distillation strategy achieves the best known bounds for the WSK capacity. Remark that, as demonstrated in Example 1, achieving the reconciliation capacity (Proposition 1), may not lead to an optimal sequential key-distillation, since the RV  $U$  that achieves  $C_{\text{rec}}(R_1, 0)$  (resp. the RVs  $U, V$  that achieve  $C_{\text{rec}}(R_1, R_2)$ ) in Proposition 1, might actually not achieve  $C_{\text{WSK}}(R_1, 0)$  (resp.  $R_{\text{WSK}}(R_1, R_2)$ ). In other words, reliability and secrecy can be handle successively, but cannot necessarily be treated as independent problems.

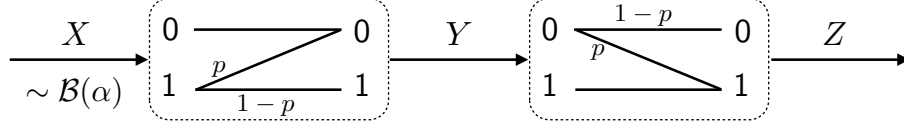


Fig. 2. Example of a binary DMS studied in Example 1

In contrast, Theorem 6 states much stronger conclusions regarding the SK capacity  $C_{SK}$ , since reconciliation and privacy amplification can be designed independently of each other in all cases. Nevertheless, in the next section we prove that for the one-way WSK capacity, reconciliation and privacy amplification can be designed independently of each other for binary or Gaussian degraded sources.

**Example 1.** Consider the scenario presented in Figure 2, in which  $X$  and  $Y$  (resp.  $Y$  and  $Z$ ) are connected by a Z-channel (resp. a mirrored Z-channel) with parameter  $p$ . Assume that  $R_1 \geq H(X|Y)$  so that

$$C_{WSK}(R_1, R_2) = \max_{p_X} (I(X; Y) - I(X; Z)), \quad C_{rec}(R_1, R_2) = \max_{p_X} I(X; Y).$$

One can check that if  $\mathbb{P}(X = 0) = \alpha$ , then  $I(X; Y) = f(\alpha) \triangleq H_b((1 - \alpha)(1 - p)) - (1 - \alpha)H_b(p)$ , and  $I(X; Z) = g(\alpha) \triangleq H_b((1 - p)(1 - \alpha + \alpha p)) - \alpha H_b(p) - (1 - \alpha)H_b(p(1 - p))$ . Numerically,  $C_{WSK}(R_1, R_2) > 0.23 > 0.22 > C_{rec}(R_1, R_2) - g(\arg\max_{\alpha} f(\alpha))$ . Hence, achieving the reconciliation capacity in a sequential key-distillation is not optimal here.

**Remark 5.** Results similar to Theorems 4, 5, 6, can be obtained by replacing extractors by hash functions. However, this incurs a communication rate loss of 1 bit, as mentioned in Section IV-B.

## V. SPECIAL CASES

In this section, we illustrate our results for a one-way rate-limited key-distillation with degraded sources, for which  $X$ ,  $Y$ , and  $Z$  form a Markov chain. With this assumption, we refine the characterization of the WSK capacity and we study sequential key-distillation for binary and Gaussian sources; in these cases, we show that reconciliation and privacy amplification can be designed independently. We also briefly discuss the performance of vector quantization compared to scalar quantization in the Gaussian case.

**Proposition 2.** Let  $(\mathcal{X}\mathcal{Y}\mathcal{Z}, p_{XYZ})$  be a MS. Assume  $X \rightarrow Y \rightarrow Z$ . For  $R_1 \in \mathbb{R}^+$ , the one-way WSK

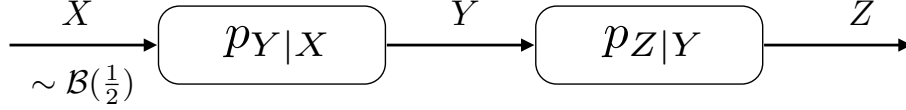


Fig. 3. Example of the DMS studied in Section V-A

capacity is

$$C_{\text{WSK}}(R_1, 0) = \max_U (I(Y; U) - I(Z; U)) \text{ subject to}$$

$$R_1 = I(X; U|Y),$$

$$U \rightarrow X \rightarrow Y \rightarrow Z,$$

$$|\mathcal{U}| \leq |\mathcal{X}| \text{ for a DMS.}$$

For a CMS, a similar result holds under the same condition as in Proposition 1.

*Proof:* See Appendix C. ■

**Remark 6.** The expression of the WSK capacity in Proposition 2 is obtained from Theorem 1.b and is due to Watanabe [16]. We refine this result by proving that equality holds in the rate constraint and by improving the range constraint of  $\mathcal{U}$ ; this refinement is critical for the analysis of binary sources, especially to solve the optimization problem for the WSK capacity in Proposition 3.

**Remark 7.** For degraded sources, and in absence of rate constraint, i.e.  $R_1 = +\infty$ , one easily shows in Theorem 4.7 of [13] that reconciliation and privacy amplification can be designed independently if and only if  $I(X; Y)$  and  $I(X; Z)$  are maximized by the same distribution  $p_X$ .<sup>4</sup> However, in Proposition 2, we can show, using [19, Proposition 2.1], that having  $I(Y; U)$  and  $I(Z; U)$  maximized by the same distribution is not sufficient, nor necessary to obtain independent reconciliation and privacy amplification.

#### A. Binary source

As depicted in Figure 3, assume that  $X$  has a Bernoulli distribution with parameter  $\frac{1}{2}$ , and that  $X \rightarrow Y \rightarrow Z$  forms a Markov chain. The alphabet  $\mathcal{X}$  is binary, but no assumption is made on  $\mathcal{Y}$  and  $\mathcal{Z}$ .

<sup>4</sup>For a DMC, it is for instance the case when the channels  $(\mathcal{X}, p_{Y|X}, \mathcal{Y})$  and  $(\mathcal{X}, p_{Z|X}, \mathcal{Z})$  are weakly symmetric [18].

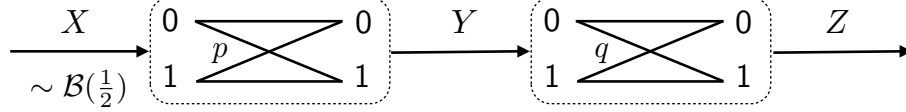


Fig. 4. Binary DMS studied in Example 2

**Proposition 3.** Let  $R_1 \in \mathbb{R}_+^*$ . If the channel  $p_{Y|X}$  and  $p_{Z|X}$  are symmetric [20], then the auxiliary RV  $U$  achieving  $C_{\text{WSK}}(R_1, 0)$  in Proposition 2, is such that the test-channel  $p_{U|X}$  is a BSC with parameter  $\beta_0$ , with  $\beta_0$ , any of the two symmetric solutions of

$$R_1 = I(U; X) - I(U; Y).$$

*Proof:* See Appendix D. ■

**Corollary 7.** Let  $R_1 \in \mathbb{R}_+^*$ . If the channel  $p_{Y|X}$  and  $p_{Z|X}$  are symmetric, then by Proposition 3, the auxiliary RV  $U$  achieving  $C_{\text{rec}}(R_1, 0)$  in Proposition 1 also achieves  $C_{\text{WSK}}(R_1, 0)$  in Proposition 2. Hence, by Propositions 1, 2 and Theorem 5, reconciliation and privacy amplification can be designed independently.

**Example 2.** As depicted in Figure 4, assume that  $X$  has a Bernoulli distribution with parameter  $\frac{1}{2}$ , and that  $X$  and  $Y$  (respectively  $Y$  and  $Z$ ) are connected by a binary symmetric channel (BSC) with crossover probability  $p$  (respectively  $q$ ). By Proposition 3, the reconciliation capacity is

$$C_{\text{rec}}(R_1, 0) = \begin{cases} 1 - H_b(p \star \beta_0), & \text{if } R_1 \leq H(X|Y), \\ 1 - H_b(p), & \text{if } R_1 \geq H(X|Y), \end{cases}$$

and the WSK capacity is

$$C_{\text{WSK}}(R_1, 0) = \begin{cases} H_b(p \star \beta_0 \star q) - H_b(p \star \beta_0), & \text{if } R_1 \leq H(X|Y), \\ H_b(p \star q) - H_b(p), & \text{if } R_1 \geq H(X|Y), \end{cases}$$

with  $\beta_0$ , any of the two symmetric solutions of the equation  $H_b(p \star \beta_0) - H_b(\beta_0) = R_1$ .

Figure 6 (resp. Figure 5) shows that the reconciliation capacity  $C_{\text{rec}}(R_1, 0)$  (resp. the secret key-capacity  $C_{\text{WSK}}(R_1, 0)$ ) is monotonically increasing in the communication rate constraint  $R_1$ . As soon as  $R_1$  is at least  $H(X|Y)$ , it attains the same maximum  $I(X; Y)$  (resp.  $I(X; Y) - I(X; Z)$ ) as in the case  $R_1 = +\infty$ .

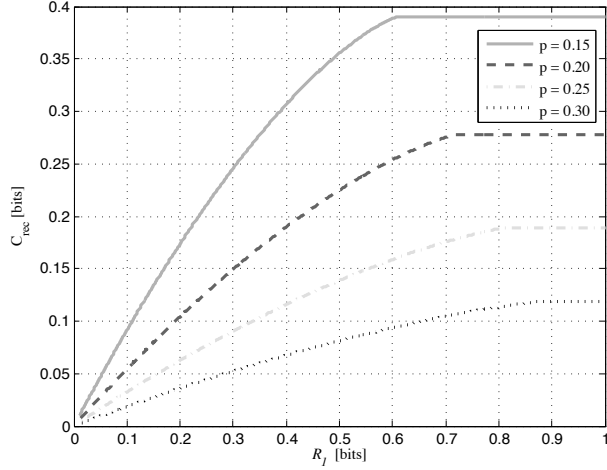
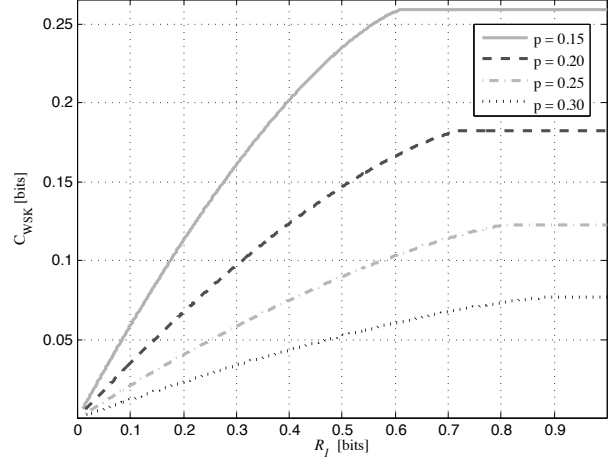
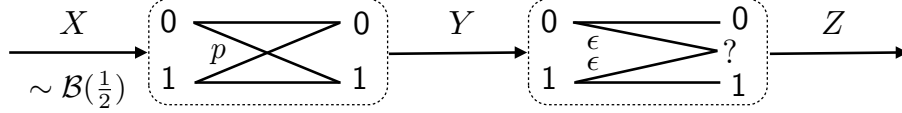
Fig. 5. Reconciliation capacity  $C_{\text{rec}}(R_1, 0)$ .Fig. 6. WSK capacity  $C_{\text{WSK}}(R_1, 0)$  ( $q = 0.2$ ).

Fig. 7. Example of the DMS studied in Example 2

Corollary 7 states that choosing a test-channel  $p_{U|X}$  as a BSC with parameter  $\beta_0$ , achieves  $C_{\text{rec}}(R_1, 0)$  and  $C_{\text{WSK}}(R_1, 0)$ , so that reconciliation and privacy amplification can be designed independently. Consequently, for any other channel  $p_{Z|Y}$ , as long as  $p_{Z|X}$  stays symmetric, the reconciliation capacity and the optimal reconciliation protocol for sequential key-distillation remains the same. It is for instance the case if we choose  $p_{Z|Y}$  as a binary erasure channel (BEC), as depicted in Figure 7. Moreover, in this case, Proposition 3 still allows us to determine the WSK capacity:

$$C_{\text{WSK}}^{(\text{erasure})}(R_1, 0) = \begin{cases} \epsilon(1 - H_b(p \star \beta_0)), & \text{if } R_1 \leq H(X|Y), \\ \epsilon(1 - H_b(p)), & \text{if } R_1 \geq H(X|Y), \end{cases}$$

where  $\epsilon$  is the erasure probability characterizing  $p_{Z|Y}$ .

### B. Gaussian sources

Let  $X$ ,  $Y$ , and  $Z$  be zero-mean correlated Gaussian sources on  $\mathbb{R}$ . Assume that Alice, Bob, and Eve know the covariance matrix of  $(X, Y, Z)$ .

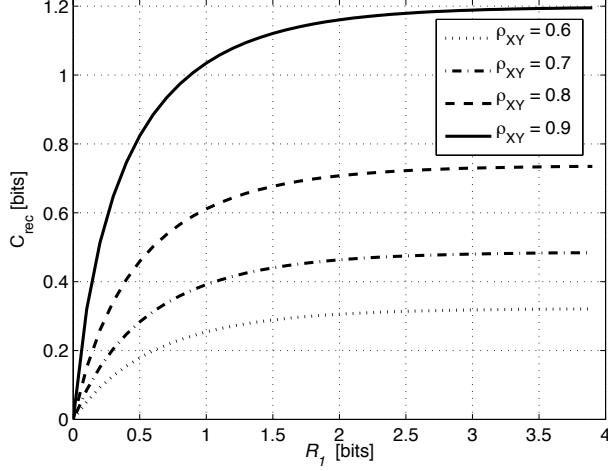


Fig. 8. Reconciliation capacity  $C_{\text{rec}}(R_1, 0)$  for different correlation coefficients  $\rho_{XY}$ .

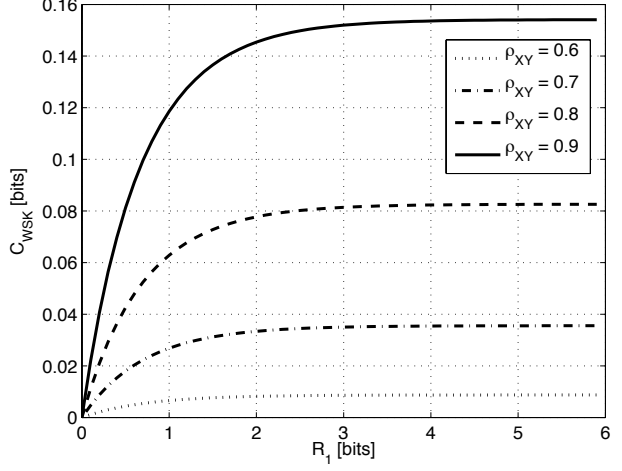


Fig. 9. WSK capacity  $C_{\text{WSK}}(R_1, 0)$ , for different correlation coefficients  $\rho_{XY}$  ( $\rho_{XZ} = 0.1$ ,  $\rho_{YZ} = 0.4$ ).

**Proposition 4.** *The auxiliary RV  $U$  achieving  $C_{\text{rec}}(R_1, 0)$  in Proposition 1 is Gaussian. Moreover, the reconciliation capacity is*

$$C_{\text{rec}}(R_1, 0) = \frac{1}{2} \log_2 \left[ \frac{1 - (\rho_{XY} e^{-R_1})^2}{1 - \rho_{XY}^2} \right],$$

where  $\rho_{XY}$  is the correlation coefficient between  $X$  and  $Y$ .

*Proof:* The result is deduced from Proposition 5 and Proposition 1. ■

**Proposition 5** ([16]). *The auxiliary RV  $U$  achieving  $C_{\text{WSK}}(R_1, 0)$  in Proposition 2 is Gaussian. Moreover, the WSK capacity is*

$$C_{\text{WSK}}(R_1, 0) = \frac{1}{2} \log_2 \left[ \frac{(1 - \rho_{YZ}^2)(1 - \rho_{XZ}^2) - (\rho_{XY} - \rho_{YZ}\rho_{XZ})^2 e^{-2R_1}}{(1 - \rho_{YZ}^2)(1 - \rho_{XZ}^2) - (\rho_{XY} - \rho_{YZ}\rho_{XZ})^2} \right].$$

As illustrated in Figure 8 (resp. Figure 9) the reconciliation capacity (resp. the WSK capacity) does not reach  $I(X; Y)$  (resp.  $I(X; Y) - I(X; Z)$ ) when  $R_1$  exceed a certain value. As mentioned in [16] and Remark 1, unlike the case of discrete random variables,  $C_{\text{rec}}(R_1, 0)$  (resp.  $C_{\text{WSK}}(R_1, 0)$ ) can only approach  $I(X; Y)$  (resp.  $I(X; Y) - I(X; Z)$ ) asymptotically. Nevertheless, we show in the next section a continuous counterpart of Remark 1.

Proposition 4 and Proposition 5 state that both arguments of the maximum for the auxiliary RV  $U$ , in Proposition 1 and in Proposition 2, are Gaussian and satisfy the same constraint  $I(X; U) - I(Y; U) = R_1$ . Since this equation has only one solution, we deduce by Propositions 1, 2 and Theorem 5 that for Gaussian

sources, achieving the reconciliation capacity in a sequential key-distillation leads to an optimal key-distillation.

### C. Practical considerations

The achievability scheme of Proposition 2 is based on Wyner-Ziv coding. For a practical implementation, additional structure needs to be introduced, for instance with vector quantization. Since scalar quantization is the simplest and often the most computationally efficient type of quantization, it is natural to ask how scalar quantization performs compared to vector quantization. We answer this question for the Gaussian case presented in Section V-B.

**Proposition 6.** *Let  $n \in \mathbb{Z}$  and  $\Delta > 0$ . Define  $U \triangleq X_Q$  a uniformly quantized version of  $X$  as follows:*

$$p_{U|Y}(u_n|y) = p_{X|Y}(t_n|y)\Delta, \quad p_U(u_n) = p_X(t_n)\Delta, \quad \text{where } t_n = \Delta/2 + (n-1)\Delta.$$

*If  $\Delta$  is small enough, then*

$$|I(X;Y) - I(Y;U)| \leq [\alpha R_1 + \beta]e^{-R_1} + K\sqrt{R_1}e^{[2(h(X|Y)-R_1)]},$$

*where  $R_1$  is the communication rate constraint, and  $\alpha, \beta, K$  are some constants.*

*Proof:* See Appendix E. ■

**Remark 8.** *The proof of Proposition 6 develops a technique that can be applied to other types of distributions (not necessarily Gaussian), as long as their pdfs exist and verify certain decreasing properties.*

Proposition 6 gives a continuous counterpart of Remark 1. Indeed, if  $R_1 > h(X|Y)$ , then we can quantize  $X$  finely enough, and Proposition 6 states that  $I(Y;U)$  approaches  $I(X;Y)$  exponentially fast as  $R_1$  increases.

Hence, vector quantization does not offer significant improvement compared to scalar quantization, when the communication rate is above  $h(X|Y)$ . Note that, in practice we can optimize the scalar quantization, so that the loss could be even smaller than predicted by Proposition 6. Figure 10 illustrates this point by comparing the reconciliation capacity with numerical values of achievable rates obtained when  $X$  is scalar-quantized.<sup>5</sup> Nevertheless, for low communication rates, Figure 10 shows that vector

<sup>5</sup>We have increased the number of interval of quantization of  $X$  from 2 to 15 and chosen their bounds by a standard gradient method to maximize  $I(X_Q;Y)$ .



quantization improves the performance; in this case, we could implement, for instance, trellis coded vector quantization (TCVQ) [21].

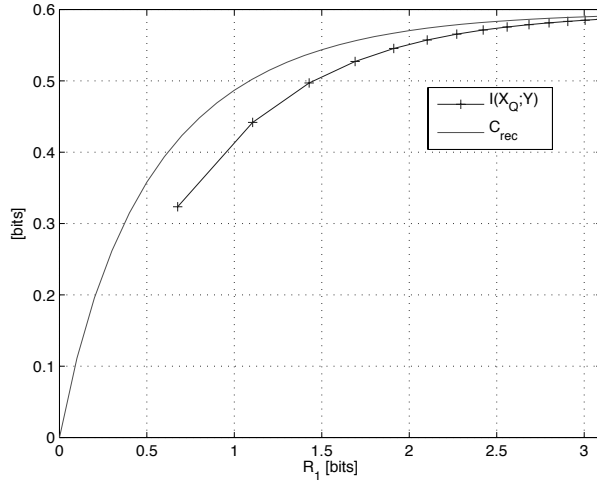


Fig. 10. Reconciliation capacity obtain with scalar quantization of  $X$  with  $\rho_{XY} = 0.75$ ,  $h(X|Y) \approx 1$ .

## VI. CONCLUDING REMARKS

We have extended the best known bounds of the WSK capacity for a discrete source model to the case of a continuous source model. For a discrete or continuous source model, we have proved that the best known bounds for the one-way WSK capacity with rate-limited public communication, are achievable by a sequential strategy that separates reliability and secrecy thanks to a reconciliation step followed by a privacy amplification step with extractors; in the case of two-way communication, the sequential design seems to suffer a loss of performance compared to the joint design and similar secret key rates were only established for degraded sources or when there is no side information at the eavesdropper (SK capacity). Moreover, we have demonstrated that reconciliation and privacy amplification can be designed independently for some scenarios, including the cases of binary and Gaussian degraded sources with one-way rate-limited public communication. A strength of sequential key-distillation is to easily translate into practical designs. Even more interestingly, the proposed scheme can be made very flexible with the following modifications.

1) *Rate-compatible reconciliation*: we can adapt to the characteristics of the legitimate users by the use of rate-compatible LDPC codes, to perform the reconciliation phase, as demonstrated in [22], [23]. Note, however, that vector quantization might be required, which could complexify the reconciliation phase.

2) *Rate-compatible privacy amplification:* In Section IV-B, we have mentioned the possible use of hash functions, if we can afford a communication rate loss of 1 bit. In the latter case, we have access to privacy amplification methods easily adjustable to the characteristics of the eavesdropper's observations, if we make  $k$  vary in the following universal family of hash functions  $\mathcal{H} = \{\text{GF}(2^n) \rightarrow \{0, 1\}^k, x \mapsto (k \text{ bits of the product } xy) | y \in \text{GF}(2^n)\}$ , where the  $k$  bits are fixed but their position can be chosen arbitrarily [24].

## APPENDIX A

### PROOF OF PROPOSITION 1

#### A. One-way communication

We first show the result for  $R_1 \in \mathbb{R}^+$  and  $R_2 = 0$ . The achievability and converse proof can be found in [15], it remains to prove that equality holds in the rate constraint (1) and that  $|\mathcal{U}| \leq |\mathcal{X}|$ .

1) *Equality constraint:* We start with the following lemma.

**Lemma 1.**  $f(U) \triangleq I(Y; U)$  and  $f_1(U) \triangleq I(X; U|Y)$  are convex in  $p_{U|X}$ .

*Proof:* Let  $\lambda \in [0, 1]$ , let  $U_1, U_2$  defined by  $p_{U_1|X}$  and  $p_{U_2|X}$  respectively, be s.t.  $U_1 \rightarrow X \rightarrow Y$  and  $U_2 \rightarrow X \rightarrow Y$ .

We introduce the random variable  $Q \in \{1, 2\}$  independent of all others and set  $U = U_Q$ .

$$Q \triangleq \begin{cases} 1 & \text{with probability } \lambda, \\ 2 & \text{with probability } 1 - \lambda. \end{cases}$$

$$\begin{aligned} I(Y; U) &\leq I(Y; UQ) \\ &= I(Y; Q) + I(Y; U|Q) \\ &\stackrel{(a)}{=} I(Y; U|Q) \\ &= \lambda I(Y; U_1) + (1 - \lambda) I(Y; U_2), \end{aligned}$$

where (a) holds since  $Y$  and  $Q$  are independent.

$$\begin{aligned} I(X; U|Y) &\leq I(X; UQ|Y) \\ &= I(X; Q|Y) + I(X; U|YQ) \\ &\stackrel{(b)}{=} I(X; U|YQ) \\ &= \lambda I(X; U_1|Y) + (1 - \lambda) I(X; U_2|Y), \end{aligned}$$

where (b) holds because  $H(X|YQ) = H(X|Y)$ , since  $Q$  and  $(X, Y)$  are independent.  $\blacksquare$

(a) *Discrete case*

By Lemma 1,  $f(U)$  and  $f_1(U)$  are convex in  $p_{U|X}$ . Define  $\Delta \triangleq \{\mathbf{u} \in \mathbb{R}^{|\mathcal{U}||\mathcal{X}|} : \forall i, j \in \llbracket 1, |\mathcal{U}| \rrbracket \times \llbracket 1, |\mathcal{X}| \rrbracket, \sum_{k=1}^{|\mathcal{U}|} u_{kj} = 1, u_{ij} \geq 0\}$ , and  $\mathcal{C} \triangleq \{\mathbf{u} \in \Delta : f_1(\mathbf{u}) \leq R_p\}$ .

We first show that  $\mathcal{C}$  is convex compact, with extreme points in  $\{\mathbf{u} \in \Delta : f_1(\mathbf{u}) = R_p\}$ :

- $\mathcal{C}$  is the preimage of  $[0, R_p]$  by the continuous function  $f_1$ , thus  $\mathcal{C}$  is closed. We deduce that  $\mathcal{C}$  is compact, since  $\mathcal{C} \subset [0, 1]^{|\mathcal{U}||\mathcal{X}|}$  and  $[0, 1]^{|\mathcal{U}||\mathcal{X}|}$  is compact.
- $\mathcal{C}$  is convex by convexity of  $f_1$ , since the sublevels of a convex function are convex sets.
- Let  $\mathbf{u}_1 \in \mathcal{C}$  s.t.  $f_1(\mathbf{u}_1) = R_p - \delta$ , with  $\delta > 0$ . By continuity of  $f_1$ ,  $\exists \epsilon_0, \forall \mathbf{u} \in \mathcal{B}(\mathbf{u}_1, \epsilon_0), |f_1(\mathbf{u}) - f_1(\mathbf{u}_1)| < \delta$ . Let  $\mathbf{u}_0 \in \mathcal{B}(\mathbf{u}_1, \epsilon_0) \setminus \{\mathbf{u}_1\}$ ,  $\lambda \in \{-\frac{1}{2}, +\frac{1}{2}\}$  and  $\mathbf{u}_\lambda = \lambda \mathbf{u}_0 + (1 - \lambda) \mathbf{u}_1$ . Then  $\|\mathbf{u}_\lambda - \mathbf{u}_1\| = \|\lambda(\mathbf{u}_0 - \mathbf{u}_1)\| \leq |\lambda| \epsilon_0$ , which means  $\mathbf{u}_\lambda \in \mathcal{C}$ . Hence,  $\frac{1}{2} \mathbf{u}_{\lambda=+1/2} + \frac{1}{2} \mathbf{u}_{\lambda=-1/2} = \mathbf{u}_1$ , and we conclude that  $\mathbf{u}_1$  is not an extreme point. Hence, the set of extreme points of  $\mathcal{C}$  is a subset of  $\{\mathbf{u} \in \Delta : f_1(\mathbf{u}) = R_p\}$ .

Since  $f$  is continuous, it reaches a maximum  $\mathbf{u}_{max}$  on the compact  $\mathcal{C}$ . Then, since  $f$  is convex and  $\mathcal{C}$  is a convex compact, by the Krein-Milman Theorem<sup>6</sup>,  $\mathbf{u}_{max}$  is a convex linear combination of extreme points of  $\mathcal{C}$  (existence of such extreme points comes directly from the Krein-Milman theorem, since  $\mathcal{C} \neq \emptyset$ ). Hence,  $\mathbf{u}_{max} = \sum_{k=1}^n \lambda_k \mathbf{u}_k$ , with  $\sum_{k=1}^n \lambda_k = 1$ ,  $\lambda_1, \lambda_2, \dots, \lambda_n \geq 0$  and  $\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_n$  extreme points of  $\mathcal{C}$ . By convexity of  $f$ ,

$$f(\mathbf{u}_{max}) \leq \sum_{k=1}^n \lambda_k f(\mathbf{u}_k) \leq \sum_{k=1}^n \lambda_k f(\mathbf{u}_{max}) = f(\mathbf{u}_{max}),$$

thus

$$\sum_{k=1}^n \lambda_k (f(\mathbf{u}_{max}) - f(\mathbf{u}_k)) = 0,$$

which means that there exists  $i \in \llbracket 1, n \rrbracket$  s.t.  $f(\mathbf{u}_{max}) = f(\mathbf{u}_i)$ . We conclude that  $\mathbf{u}_{max}$  is an extreme point of  $\mathcal{C}$ . This result is known as the maximum principle [25].

(b) *Continuous case*

If the probability density functions (pdf)  $f_{U|X}$  and  $f_{V|YU}$  exist and are in  $(\mathcal{B}_c(K), \|\cdot\|_\infty)$ , the set of  $K$ -bounded continuous function, where  $K \in \mathbb{R}$ , then we proceed as in the discrete case by using the theorem in [26] instead of Krein-Milman Theorem, since  $\mathcal{B}_c(K)$  has the positive binary intersection [27].

<sup>6</sup> A compact convex subset of a locally convex topological vector space is the closed convex hull of the set of its extreme points. Actually, only a weaker version is used since a finite dimensional space is considered.

2) *Cardinality bound*  $|\mathcal{U}| \leq |\mathcal{X}|$ : This result is a special case of a more general one that we prove in Appendix C-B.

### B. Two-way communication

Let  $R_1, R_2 \in \mathbb{R}^+$ .

1) *Converse*: We first establish the rate constraints on  $R_1$  and  $R_2$ . We have

$$\begin{aligned}
 nR_1 &\geq H(A) \\
 &\geq I(A; X^n) - I(A; Y^n) \\
 &\stackrel{(a)}{=} n[I(A; X_J|\tilde{U}) - I(A; Y_J|\tilde{U})] \\
 &\stackrel{(b)}{=} n[I(U; X_J) - I(U; Y_J)] \\
 &\stackrel{(c)}{=} nI(U; X_J|Y_J)
 \end{aligned} \tag{8}$$

where (a) holds by [28, Lemma 4.1], if we set  $\tilde{U} = X^{J-1}Y_{J+1}^N J$  and  $J$  is a **RV** uniformly distributed on  $\llbracket 1, n \rrbracket$ , independent of all previous **RVs**, (b) holds if we set  $U = A\tilde{U}$ , since  $X_J$  and  $\tilde{U}$  are independent, and (c) holds since  $U \rightarrow X_J \rightarrow Y_J$  forms a Markov chain. Similarly, we have

$$\begin{aligned}
 nR_2 &\geq H(B|A) \\
 &\stackrel{(d)}{\geq} H(B|X^n) + H(\hat{S}|S) - n\delta(\epsilon) \\
 &\stackrel{(e)}{\geq} I(\hat{S}; B|X^n) + H(\hat{S}|BX^n) - n\delta(\epsilon) \\
 &= H(\hat{S}|X^n) - n\delta(\epsilon) \\
 &= H(\hat{S}|A) - I(\hat{S}; X^n|A) - n\delta(\epsilon) \\
 &\stackrel{(f)}{=} I(\hat{S}; Y^n|A) - I(\hat{S}; X^n|A) - n\delta(\epsilon) \\
 &\stackrel{(g)}{=} n[I(V; Y_J|U) - I(V; X_J|U)] - n\delta(\epsilon) \\
 &\stackrel{(h)}{=} nI(UV; Y_J|X_J) - n\delta(\epsilon),
 \end{aligned} \tag{9}$$

where (d) holds because  $A$  is a function of  $X^n$  and by Fano's inequality, since for any  $\epsilon > 0$ , there exists a reconciliation protocol such that  $\mathbb{P}(S \neq \hat{S}) \leq \delta(\epsilon)$ ,<sup>7</sup> (e) holds since  $S = \eta_a(X^n, B)$ , (f) holds since  $\hat{S} = \eta_b(Y^n, A)$ , (g) holds by [28, Lemma 4.1] and if we set  $V = \hat{S}$ , finally (h) holds since

<sup>7</sup> $\delta(\epsilon)$  denotes a function of  $\epsilon$  such that  $\lim_{\epsilon \rightarrow 0} \delta(\epsilon) = 0$ .

$V \rightarrow Y_J U \rightarrow X_J$  and  $U \rightarrow X_J \rightarrow Y_J$ .

We now determine the reconciliation capacity bound.

$$\begin{aligned}
I(\hat{S}; X^n) &= \sum_{i=1}^n I(\hat{S}; X_i | X^{i-1}) \\
&\stackrel{(a)}{=} \sum_{i=1}^n I(\hat{S} X^{i-1}; X_i) \\
&\leq \sum_{i=1}^n I(\hat{S} X^{i-1} Y_{i+1}^n; X_i) \\
&= n \sum_{i=1}^n \mathbb{P}(J = i) I(\hat{S} X^{J-1} Y_{J+1}^n; X_J | J = i) \\
&= n I(\hat{S} \tilde{U}; X_J | J) \\
&\leq n I(VU; X_J),
\end{aligned} \tag{10}$$

where (a) holds because the  $X_i$ 's are i.i.d.. Then,

$$\begin{aligned}
H(\hat{S}) - H(AB) &= I(\hat{S}; X^n) + H(\hat{S} | X^n) - H(A) - H(B|A) \\
&\stackrel{(b)}{\leq} n I(VU; X_J) - H(A) + n \delta(\epsilon) \\
&\stackrel{(c)}{=} n [I(VU; X_J) - I(U; X_J | Y_J) + \delta(\epsilon)] \\
&= n [I(X_J; Y_J) - I(X_J; Y_J | UV) + \delta(\epsilon)],
\end{aligned}$$

where (b) holds by (10) and since  $H(\hat{S} | X^n) \leq H(B|A) + n \delta(\epsilon)$  by (9), and (c) holds by (8).

For a DMS, standard techniques [28] show that  $|\mathcal{U}| \leq |\mathcal{X}| + 2$  and  $|\mathcal{V}| \leq |\mathcal{Y}|$ .

2) *Achievability:* The proof for a DMS is similar to Wyner-Ziv coding [29], we only describe the protocol. In the following, for  $n \in \mathbb{N}$  and  $\epsilon > 0$ , we note  $T_\epsilon^n(X)$  the set of  $\epsilon$ -letter-typical sequences [30] (also called “robustly typical sequence” in [31]) with respect to  $p_X$ . We also define conditional typical sets as follows,  $T_\epsilon^n(Y|x^n) \triangleq \{y^n : (x^n, y^n) \in T_\epsilon^n(XY)\}$ . We note  $\mu_X \triangleq \min_{x \in \text{supp}(p_X)} p_X(x)$ . Let  $\epsilon > 0$ , and define  $\epsilon_1 \triangleq \frac{1}{2}\epsilon$ ,  $\epsilon_2 \triangleq 2\epsilon$ .

**Code construction:** Fix a joint probability distribution  $p_{UX}$  on  $\mathcal{U} \times \mathcal{X}$  and  $p_{UVY}$  on  $\mathcal{U} \times \mathcal{V} \times \mathcal{Y}$ . Let  $R_u = I(X; U|Y) + 6\epsilon H(U)$ ,  $R'_u = I(Y; U) - 3\epsilon H(U)$ . Generate  $2^{n(R_u + R'_u)}$  codewords, labeled  $u^n(\omega, \nu)$  with  $(\omega, \nu) \in \llbracket 1, 2^{nR_u} \rrbracket \times \llbracket 1, 2^{nR'_u} \rrbracket$ , by generating the symbols  $u_i(\omega, \nu)$  for  $i \in \llbracket 1, n \rrbracket$  and  $(\omega, \nu) \in \llbracket 1, 2^{nR_u} \rrbracket \times \llbracket 1, 2^{nR'_u} \rrbracket$  independently according to  $p_U$ . Let  $R_v = I(V; Y|XU) + 6\epsilon_2 H(V|U)$ ,  $R'_v = I(V; X|U) - 3\epsilon_2 H(V|U)$ . For each  $(\omega, \nu)$ , generate  $2^{n(R_v + R'_v)}$  codewords, labeled  $v^n(\omega, \nu, k, l)$  with  $(k, l) \in \llbracket 1, 2^{nR_v} \rrbracket \times \llbracket 1, 2^{nR'_v} \rrbracket$ , by generating the symbols  $v_i(\omega, \nu, k, l)$  for  $i \in \llbracket 1, n \rrbracket$  and  $(k, l) \in$

$\llbracket 1, 2^{nR_v} \rrbracket \times \llbracket 1, 2^{nR'_v} \rrbracket$  independently according to  $p_{V|U=u_i(\omega, \nu)}$ .

**Step1. At Alice's side:** Given  $x^n$ , find a pair  $(\omega, \nu)$  s.t.  $(x^n, u^n(\omega, \nu)) \in T_\epsilon^n(XU)$ . If we find several pairs, we choose the smallest one (by lexicographic order). If we fail we choose  $(\omega, \nu) = (1, 1)$ . Define  $s_1^n \triangleq u^n(\omega, \nu)$  and transmit  $a^n \triangleq \omega$ .

**Step2. At Bob's side:** Given  $y^n$  and  $a^n$ , find  $\tilde{\nu}$  s.t.  $(y^n, u^n(\omega, \tilde{\nu})) \in T_\epsilon^n(YU)$  and define  $\hat{s}_1^n \triangleq u^n(\omega, \tilde{\nu})$ . If there is one or more such  $\tilde{\nu}$ , choose the lowest, otherwise set  $\tilde{\nu} = 1$ . Find a pair  $(k, l)$  such that  $(\hat{s}_1^n, y^n, v^n(\omega, \tilde{\nu}, k, l)) \in T_{\epsilon_2}^n(UYV)$ . If there is one or more such  $(k, l)$ , choose the lowest, otherwise set  $(k, l) = (1, 1)$ . Transmit  $b^n = k$ . Define  $\hat{s}_2^n \triangleq v^n(\omega, \tilde{\nu}, k, l)$  and  $\hat{s}^n \triangleq (\hat{s}_1^n, \hat{s}_2^n)$ .

**Step3. At Alice's side:** Given  $s_1^n = u^n(\omega, \nu)$  and  $b^n$ , find  $\tilde{l}$  s.t.  $(x^n, s_1^n, v^n(\omega, \tilde{\nu}, k, \tilde{l})) \in T_{\epsilon_2}^n(XUV)$ . If there is one or more such  $\tilde{l}$ , choose the lowest, otherwise set  $\tilde{l} = 1$ . Define  $s_2^n \triangleq v^n(\omega, \tilde{\nu}, k, \tilde{l})$  and  $s^n \triangleq (s_1^n, s_2^n)$ .

We can show by standard arguments that there exists a code, such that after one repetition of the protocol, Alice obtains  $S^n = U^n \hat{V}^n$ , whereas Bob has  $\hat{S}^n = \hat{U}^n V^n$  with  $\mathbb{P}[\hat{U}^n \neq U^n] \leq \delta_\epsilon(n)$ ,<sup>8</sup>  $\mathbb{P}[\hat{V}^n \neq V^n] \leq \delta_\epsilon(n)$ ,  $\mathbb{P}[\hat{S}^n \neq S^n | \mathcal{R}_n] \leq P_e(\epsilon, n)$ <sup>9</sup> and  $(U^n, X^n), (\hat{U}^n, Y^n), (\hat{U}^n, Y^n, V^n), (U^n, \hat{V}^n, X^n)$  jointly typical with probability approaching one for  $n$  large.

To extend the result to a CMS, we proceed as in the proof of Theorem 4.

## APPENDIX B

### PROOFS FOR SECTION IV-C

#### A. Proof of Theorem 4

In the following, we use the same notations as in Appendix A.

1) *Discrete case:* Let  $\epsilon > 0$ . Let  $R_1, R_2 \in \mathbb{R}^+$ . Let  $m, n \in \mathbb{N}$ , and define  $N \triangleq nm$ . Let  $k \in \mathbb{N}$  to be determined later. Consider a sequential key-distillation strategy  $\mathcal{S}_N$  that consists of

- $m$  repetitions of a reconciliation protocol  $\mathcal{R}_n$  based on Wyner-Ziv coding. One protocol operates as described in Appendix A-B. Hence, after one repetition of the protocol,  $\mathbb{P}[\hat{S}^n \neq S^n | \mathcal{R}_n] \leq P_e(\epsilon, n)$ . In addition, the information disclosed over the public channel during the  $m$  repetition of the reconciliation protocol is upper bounded by  $\log|\mathcal{A}|^N + \log|\mathcal{B}|^N = NI(U; X|Y) + NI(V; Y|XU) + Nr_0(\epsilon)$ , with  $\lim_{\epsilon \rightarrow 0} r_0(\epsilon) = 0$ ;<sup>10</sup>

<sup>8</sup> $\delta_\epsilon(n)$  denotes a function of  $\epsilon$  and  $n$  such that  $\lim_{n \rightarrow \infty} \delta_\epsilon(n) = 0$ .

<sup>9</sup>In Appendix F we show that  $P_e(\epsilon, n)$  decreases exponentially to zero as  $n\epsilon^2$  goes to infinity.

<sup>10</sup> $r_0 \triangleq O(\epsilon H(UV))$ .

- privacy amplification based on extractors, with output size  $k$ , at the end of which Alice computes her key  $K = g(S^N, U_d)$ , while Bob computes  $\hat{K} = g(\hat{S}^N, U_d)$ , where  $U_d$  is a sequence of  $d$  uniformly distributed random bits.

The total information available to Eve after reconciliation consists of her observation  $Z^N$ , the public messages  $A^N$  and  $B^N$ , respectively sent by Alice and Bob, and  $U_d$ . The strategy  $\mathcal{S}_N$  is also known to Eve, but we omit the conditioning on  $\mathcal{S}_N$  for convenience.

We first show that, for a suitable choice of the output size  $k$ , we have  $k \geq H(K|U_d Z^N A^N B^N) \geq k - \delta(N)$ .<sup>11</sup> Then, we show that the corresponding WSK rate achieves the lower bound on the WSK capacity of Theorem 1. We first state Lemma 2, a refined version of the results in [9], [13], that is obtained by using the notion of robust typicality developed in the appendix of [31], to later extend our result to the continuous case.

**Lemma 2** ([9], [13], Refined version). *Consider a DMS  $(\mathcal{XZ}, p_{XZ})$  and define the RV  $\Theta$  as*

$$\Theta \triangleq \begin{cases} 1 & \text{if } (X^n, Z^n) \in \mathcal{T}_{2\epsilon}^n(XZ) \text{ and } Z^n \in \mathcal{T}_\epsilon^n(Z), \\ 0 & \text{otherwise.} \end{cases}$$

*Then,  $\mathbb{P}[\Theta = 1] \geq 1 - \delta_\epsilon^0(n)$ , with  $\delta_\epsilon^0(n) \triangleq 4|S_X|e^{-\epsilon^2 n \mu_X/3}$ , where  $S_X = \{x \in \mathcal{X} : p(x) > 0\}$  and  $\mu_X = \min_{x \in S_X} p(x)$ . Moreover, if  $z^n \in \mathcal{T}_\epsilon^n(Z)$ ,*

$$H_\infty(X^n|Z^n = z^n, \Theta = 1) \geq n(H(X|Z) - \delta(\epsilon)) - \delta_\epsilon^1(n), \text{ where } \delta_\epsilon^1(n) \triangleq 4|S_{X,Y}|e^{-\epsilon^2 n \mu_{X,Y}/6}.$$

Let us start by defining the following RVs

$$\Theta \triangleq \begin{cases} 1 & \text{if } (S^N, Z^N) \in \mathcal{T}_{2\epsilon}^m(S^N Z^N) \text{ and } Z^N \in \mathcal{T}_\epsilon^m(Z^N), \\ 0 & \text{otherwise.} \end{cases}$$

$$\Upsilon \triangleq \begin{cases} 1 & \text{if } H_\infty(S^N|Z^N, a^N, b^N, \Theta = 1) \leq \log(|\mathcal{A}|^N |\mathcal{B}|^N) + \sqrt{N}, \\ 0 & \text{otherwise.} \end{cases}$$

By Lemma 2 applied to the DMS  $(\mathcal{U}^N \mathcal{V}^N \mathcal{Z}^N, p_{S^N Z^N})$ ,  $\mathbb{P}(\Theta = 1) \geq 1 - \delta_\epsilon^0(m)$ , and by [9, Lemma 10],  $\mathbb{P}(\Upsilon = 1) \geq 1 - 2^{-\sqrt{N}}$ . Hence,  $\mathbb{P}(\Upsilon = 1, \Theta = 1) \geq 1 - \delta_\epsilon^0(m) - 2^{-\sqrt{N}}$ , and

$$H(K|U_d Z^N A^N B^N) \geq \left(1 - \delta_\epsilon^0(m) - 2^{-\sqrt{N}}\right) H(K|U_d Z^N A^N B^N, \Upsilon = 1, \Theta = 1). \quad (11)$$

<sup>11</sup> $\delta(n)$  denotes a function of  $n$  such that  $\lim_{n \rightarrow \infty} \delta(n) = 0$ .

To lower bound  $H(K|U_d Z^N A^N B^N, \Upsilon = 1, \Theta = 1)$ , we first lower bound  $H_\infty(S^N|Z^N = z^N, A^N = a^N, B^N = b^N, \Theta = 1, \Upsilon = 1)$  to be able to use Theorem 3. By definition of  $\Upsilon$ ,

$$\begin{aligned} & H_\infty(S^N|Z^N = z^N, A^N = a^N, B^N = b^N, \Theta = 1, \Upsilon = 1) \\ & \geq H_\infty(S^N|Z^N = z^N, \Theta = 1) - \log(|\mathcal{A}|^N |\mathcal{B}|^N) - \sqrt{N} \\ & \stackrel{(a)}{\geq} m(H(S^n|Z^n) - \delta(\epsilon)) - \delta_\epsilon^1(m) - N(I(U; X|Y) + I(V; Y|XU)) - \sqrt{N} - Nr_0(\epsilon), \end{aligned} \quad (12)$$

where (a) follows from Lemma 2,<sup>12</sup> and  $\log(|\mathcal{A}|^N |\mathcal{B}|^N) = N(I(U; X|Y) + I(V; Y|XU)) + Nr_0(\epsilon)$ . We now lower bound  $H(S^n|Z^n)$ . We first remark that

$$\begin{aligned} H(S^n|Z^n) &= H(\hat{S}^n|Z^n) + H(S^n|\hat{S}^n Z^n) - H(\hat{S}^n|S^n Z^n) \\ &\stackrel{(a)}{\geq} H(\hat{S}^n|Z^n) - \delta_\epsilon(n) \\ &= I(Y^n; \hat{S}^n|Z^n) + H(\hat{S}^n|Y^n Z^n) - \delta_\epsilon(n) \\ &= H(Y^n|Z^n) - H(Y^n|Z^n \hat{S}^n) + H(\hat{U}^n|Y^n Z^n) + H(V^n|Y^n \hat{U}^n Z^n) - \delta_\epsilon(n) \\ &\stackrel{(b)}{=} nH(Y|Z) + H(\hat{U}^n|Y^n Z^n) - H(Y^n|Z^n \hat{S}^n) - \delta_\epsilon(n), \end{aligned} \quad (13)$$

where (a) is from Fano's inequality and (b) holds because  $V^n$  is a function of  $(Y^n \hat{U}^n)$ , the  $Y_i$ 's and  $Z_i$ 's are i.i.d.. We first lower bound  $H(\hat{U}^n|Y^n Z^n)$ . Remark that

$$\begin{aligned} H(\hat{U}^n|Y^n Z^n) &= H(U^n|Y^n Z^n) + H(\hat{U}^n|U^n Y^n Z^n) - H(U^n|\hat{U}^n Y^n Z^n) \\ &\stackrel{(c)}{\geq} H(U^n|Y^n Z^n) - \delta_\epsilon(n) \\ &= I(X^n; U^n|Y^n Z^n) + H(U^n|X^n Y^n Z^n) - \delta_\epsilon(n) \\ &\stackrel{(d)}{=} I(X^n; U^n|Y^n Z^n) - \delta_\epsilon(n) \\ &= H(X^n|Y^n Z^n) - H(X^n|Y^n Z^n U^n) - \delta_\epsilon(n) \\ &\stackrel{(e)}{=} nH(X|YZ) - H(X^n|Y^n Z^n U^n) - \delta_\epsilon(n), \end{aligned} \quad (14)$$

<sup>12</sup>The  $m$  repetitions of the protocol  $\mathcal{R}_n$  allow us to link  $H_\infty(\cdot)$  to  $H(\cdot)$ .



where (c) is from Fano's inequality, (d) holds because  $U^n$  is a function of  $X^n$  ( $U^n$  is a quantized version of  $X^n$ ), and (e) is true since the  $X_i$ 's,  $Y_i$ 's, and  $Z_i$ 's are i.i.d.. Then, define

$$\Gamma \triangleq \begin{cases} 1 & \text{if } (X^n, U^n, (YZ)^n) \in \mathcal{T}_{2\epsilon}^n(XUYZ), \\ 0 & \text{otherwise.} \end{cases}$$

$$\Delta \triangleq \begin{cases} 1 & \text{if } (X^n, U^n) \in \mathcal{T}_\epsilon^n(XU), \\ 0 & \text{otherwise.} \end{cases}$$

so that,

$$\begin{aligned} H(X^n|Y^n Z^n U^n) &\leq H(X^n \Gamma \Delta | Y^n Z^n U^n) \\ &= H(\Gamma \Delta | Y^n Z^n U^n) + H(X^n | Y^n Z^n U^n \Gamma \Delta) \\ &\leq 2 + \sum_{\delta, \gamma \in \{0,1\}} \mathbb{P}(\Gamma = \gamma | \Delta = \delta) \mathbb{P}(\Delta = \delta) \times H(X^n | Y^n Z^n U^n, \Gamma = \gamma, \Delta = \delta) \\ &\stackrel{(f)}{\leq} 2 + H(X^n | Y^n Z^n U^n, \Gamma = 1, \Delta = 1) + n(2\delta_\epsilon^2(n) + \delta_\epsilon^4(n)/2) \log |\mathcal{X}|, \end{aligned} \quad (15)$$

where (f) holds since  $\mathbb{P}(\Delta = 0) \leq \delta_\epsilon^2(n)$ ,<sup>13</sup> and  $\mathbb{P}(\Gamma = 0 | \Delta = 1) \leq \delta_\epsilon^4(n)/2$ .<sup>14</sup> Indeed, we can apply Markov Lemma [32] (see the version given in [31]), since we have  $U^n \rightarrow X^n \rightarrow Y^n Z^n$  and for every  $(x^n, (yz)^n)$ ,  $p((yz)^n | x^n) = \prod_{i=1}^n p_{YZ|X}(y_i z_i | x_i)$ . Then,

$$\begin{aligned} H(X^n | Y^n Z^n U^n, \Gamma = 1, \Delta = 1) &= \sum_{y^n, z^n, u^n} p(y^n, z^n, u^n | 1, 1) \times H(X^n | y^n, z^n, u^n, \Gamma = 1, \Delta = 1) \\ &\leq \sum_{y^n, z^n, u^n} p(y^n, z^n, u^n | 1, 1) \log |\mathcal{T}_{2\epsilon}^n(X | y^n, z^n, u^n)| \\ &\leq \sum_{y^n, z^n, u^n} p(y^n, z^n, u^n | 1, 1) (nH(X | YZU)(1 + 2\epsilon)) \\ &\leq nH(X | YZU)(1 + 2\epsilon). \end{aligned} \quad (16)$$

Hence, combining (14), (15), and (16), we obtain

$$H(\hat{U}^n | Y^n Z^n) \geq nH(X | YZ) - nH(X | YZU) - r_1(\epsilon, n), \quad (17)$$

where

$$r_1(\epsilon, n) \triangleq 2nH(X | YZU)\epsilon + n(2\delta_\epsilon^2(n) + \delta_\epsilon^4(n)/2) \log |\mathcal{X}| + 2 + \delta_\epsilon(n). \quad (18)$$

<sup>13</sup>We have  $\delta_\epsilon^2(n) \leq P_e(\epsilon, n)$  by Wyner-Ziv coding in the reconciliation protocols.

<sup>14</sup>By Markov Lemma, we have  $\delta_\epsilon^4(n) \triangleq 2|S_{XYZ}|e^{-\epsilon^2 n \mu_{XYZ}/6}$ .

We now lower bound the term  $-H(Y^n|Z^n\hat{S}^n)$  in (13). Define

$$\Gamma_1 \triangleq \begin{cases} 1 & \text{if } (Y^n\hat{U}^n, V^n, Z^n) \in T_{2\epsilon}^n((Y\hat{U})VZ), \\ 0 & \text{otherwise.} \end{cases}$$

$$\Delta_1 \triangleq \begin{cases} 1 & \text{if } (Y^n\hat{U}^n, V^n) \in T_\epsilon^n((Y\hat{U})V), \\ 0 & \text{otherwise.} \end{cases}$$

We can write

$$\begin{aligned} H(Y^n|Z^n\hat{S}^n) &\leq H(Y^n\Gamma_1\Delta_1|Z^n\hat{S}^n) \\ &= H(\Gamma_1\Delta_1|Z^n\hat{S}^n) + H(Y^n|Z^n\hat{S}^n\Gamma_1\Delta_1) \\ &\leq 2 + \sum_{\delta_1, \gamma_1 \in \{0,1\}} \mathbb{P}(\Gamma_1 = \gamma_1 | \Delta_1 = \delta_1) \mathbb{P}(\Delta_1 = \delta_1) H(Y^n|Z^n\hat{S}^n, \Gamma_1 = \gamma_1, \Delta_1 = \delta_1) \\ &\stackrel{(g)}{\leq} 2 + H(Y^n|Z^n\hat{S}^n, \Gamma_1 = 1, \Delta_1 = 1) + n(2\delta_\epsilon^3(n) + \delta_\epsilon^5(n)/2) \log|\mathcal{Y}|, \end{aligned} \quad (19)$$

where (g) holds since  $\mathbb{P}(\Delta_1 = 0) \leq \delta_\epsilon^3(n)$ ,<sup>15</sup> and  $\mathbb{P}(\Gamma_1 = 0 | \Delta_1 = 1) \leq \delta_\epsilon^5(n)/2$ .<sup>16</sup> Indeed, we can apply Markov Lemma (see the version in [31]), since we have  $V^n \rightarrow Y^n\hat{U}^n \rightarrow Z^n$  and for every  $((y\hat{u})^n, z^n)$ ,  $p(z^n|y^n\hat{u}^n) = p(z^n|y^n) = \prod_{i=1}^n p_{Z|Y}(z_i|y_i) = \prod_{i=1}^n p_{Z|YU}(z_i|y_i\hat{u}_i)$ , because  $\hat{U}^n \rightarrow Y^n \rightarrow Z^n$  if  $X^n \rightarrow Y^n \rightarrow Z^n$ <sup>17</sup>. Then,

$$\begin{aligned} &H(Y^n|Z^n\hat{S}^n, \Gamma_1 = 1, \Delta_1 = 1) \\ &= \sum_{z^n, \hat{s}^n} p(z^n, \hat{s}^n | 1, 1) H(Y^n|Z^n = z^n, \hat{S}^n = \hat{s}^n, \Gamma_1 = 1, \Delta_1 = 1) \\ &\leq \sum_{z^n, \hat{s}^n} p(z^n, \hat{s}^n | 1, 1) \log|T_{2\epsilon}^n(Y|z^n, \hat{s}^n)| \\ &\leq \sum_{z^n, \hat{s}^n} p(z^n, \hat{s}^n | 1, 1) (nH(Y|ZUV)(1 + 2\epsilon)) \\ &\leq nH(Y|ZUV)(1 + 2\epsilon). \end{aligned} \quad (20)$$

<sup>15</sup>We have  $\delta_\epsilon^3(n) \leq P_e(\epsilon, n)$  by Wyner-Ziv coding in the reconciliation protocols.

<sup>16</sup>By Markov Lemma, we have  $\delta_\epsilon^5(n) \triangleq 2|S_{YUZ}|e^{-\epsilon^2 n \mu_{YUZ}/6}$ .

<sup>17</sup>Note that the assumption of degraded sources is only necessary here. The use of this hypothesis is the weakness, at least for two-way communication (for one-way communication this assumption is not necessary), of a proof that consists of a successive design of reconciliation and privacy amplification, rather than a joint design as in [3], where they exploit the joint design to get the joint typicality of  $(V^n, Y^n, U^n, Z^n)$ .

Hence by (19), (20),

$$H(Y^n|Z^n U^n V^n) \leq nH(Y|ZUV) + r_2(\epsilon, n), \quad (21)$$

where

$$r_2(\epsilon, n) \triangleq 2nH(Y|ZUV)\epsilon + n(2\delta_\epsilon^3(n) + \delta_\epsilon^5(n)/2) \log|\mathcal{Y}| + 2. \quad (22)$$

Combining (13), (17), (21),

$$H(S^n|Z^n) \geq n[H(Y|Z) + H(X|YZ) - H(X|YZU) - H(Y|ZUV)] - r_1(\epsilon, n) - r_2(\epsilon, n) - \delta_\epsilon(n). \quad (23)$$

Then, remark that

$$\begin{aligned} & H(Y|Z) + H(X|YZ) - H(X|YZU) - H(Y|ZUV) \\ &= I(Y; UV|Z) + I(X; U|YZ) \\ &= H(UV|Z) - H(UV|YZ) + I(X; U|YZ) \\ &= H(U|Z) + H(V|UZ) - H(U|YZ) - H(V|UYZ) + I(X; U|YZ) \\ &\stackrel{(h)}{\geq} H(U|Z) - I(V; Z|U) + H(V|U) - H(U|YZ) - H(V|UY) + I(X; U|YZ) \\ &= H(U|Z) - I(V; Z|U) - H(U|YZ) + I(V; Y|U) + I(X; U|YZ) \\ &\stackrel{(i)}{\geq} H(U|Z) - I(V; Z|U) - H(U|YZ) + I(V; Y|U) - H(U|X) + H(U|YZ) \\ &= I(U; X) - I(U; Z) - I(V; Z|U) + I(V; Y|U), \end{aligned} \quad (24)$$

where (h) and (i) holds because conditioning reduces entropy. Hence, by (12), (23) and (24)

$$\begin{aligned} & H_\infty(S^N|Z^N = z^N, A^N = a^N, B^N = b^N, \Theta = 1, \Upsilon = 1) \\ &\geq N[I(U; Y) + I(V; X|U) - I(U; Z) - I(V; Z|U)] - r_3(\epsilon, N), \end{aligned} \quad (25)$$

where

$$r_3(\epsilon, N) \triangleq m(r_1(\epsilon, n) + r_2(\epsilon, n) + \delta_\epsilon(n) + \delta(\epsilon)) + \delta_\epsilon^1(m) + Nr_0(\epsilon) + \sqrt{N}. \quad (26)$$

Set  $k$  to be less than the lower bound in (25) by  $\sqrt{N}$ :

$$k \triangleq \lfloor N[I(U; Y) + I(V; X|U) - I(U; Z) - I(V; Z|U)] - r_3(\epsilon, N) - \sqrt{N} \rfloor. \quad (27)$$

Now that we have lower bounded  $H_\infty(S^N|Z^N = z^N, A^N = a^N, B^N = b^N, \Theta = 1, \Upsilon = 1)$  in (25) by  $k$  (defined in (27)), we can apply Theorem 3 to lower bound  $H(K|U_d Z^N A^N B^N, \Upsilon = 1, \Theta = 1)$  by  $k -$

$N\delta^*(N)$ , where  $\delta^*(N)$  is defined in the theorem. Thus, we can finally lower bound  $H(K|U_d Z^N A^N B^N)$  in (11):

$$H(K|U_d Z^N A^N B^N) \geq \left(1 - \delta_\epsilon^0(m) - 2^{-\sqrt{N}}\right) (k - N\delta^*(N)) = k - \delta(N),$$

where the equality is obtained thanks to the exponential decrease of  $\delta^*$  and  $\delta_\epsilon^0$ . Moreover, the leakage is such that

$$I(K; U_d Z^N A^N B^N) = H(K) - H(K|U_d Z^N A^N B^N) \leq \delta(N). \quad (28)$$

The keys computed by Alice and Bob are asymptotically the same as  $N$  goes to infinity, since

$$\mathbb{P}(K \neq \hat{K}) \leq \mathbb{P}(S^N \neq \hat{S}^N) \leq m\mathbb{P}((U^n \hat{V}^n) \neq (\hat{U}^n V^n)) \leq mP_e(\epsilon, n). \quad (29)$$

Then, by (18), (22), (26), we have that  $r_3(\epsilon, N)/N = \delta(N) + \delta(\epsilon)$ , thus the secret key rate  $R \triangleq k/N$  is

$$R = I(U; Y) - I(U; Z) + I(V; X|U) - I(V; Z|U) - \delta(\epsilon) - \delta(N).$$

Note that it is not exactly the bound proposed in Theorem 1.a for the WSK capacity. We finish the proof as follows. If  $I(V; X|U) \leq I(V; Z|U)$ , in the reconciliation we set  $R_2 = 0$  so that we now have

$$R = I(U; Y) - I(U; Z) + [I(V; X|U) - I(V; Z|U)]^+ - \delta(\epsilon) - \delta(N).$$

Then, if  $I(U; Y) \leq I(U; Z)$ , in the reconciliation protocol, we choose  $S^n = V^n$  (see the beginning of the proof), and we assume that  $U^N$  is provided by a genie to Eve. Consequently, we obtain instead of Equation (12),

$$\begin{aligned} H_\infty(V^N | Z^N = z^N, U^N = u^N, B = b, \Theta = 1, \Upsilon = 1) \\ \geq m(H(V^n | Z^n U^n) - \delta(\epsilon)) - \delta_\epsilon^1(m) - NI(V; Y | XU) - \sqrt{N} - Nr_0(\epsilon), \end{aligned}$$

and conclude in the same manner, to obtain

$$R = [I(U; Y) - I(U; Z)]^+ + [I(V; X|U) - I(V; Z|U)]^+ - \delta(\epsilon) - \delta(N).$$

2) *Continuous case:* We use the following lemma to extend the result to the continuous case.

**Lemma 3** ([33], [34], [35]). *Let  $X$  and  $Y$  be two real-valued random variables with probability distribution  $\mathbb{P}_X$  and  $\mathbb{P}_Y$  respectively. Let  $\mathcal{E}_{\Delta_1} = \{E_i\}_{i \in \mathcal{I}}$ ,  $\mathcal{F}_{\Delta_2} = \{F_j\}_{j \in \mathcal{J}}$  be two partitions of  $X$  and  $Y$  such that for any  $i \in \mathcal{I}$ ,  $\mathbb{P}_X(E_i) = \Delta_1$ , for any  $j \in \mathcal{J}$ ,  $\mathbb{P}_Y(F_j) = \Delta_2$ , where  $\Delta_1, \Delta_2 > 0$ . Let*

$X_{\Delta_1}, Y_{\Delta_2}$  be the quantized version of  $X, Y$  with respect to the partitions  $\mathcal{E}_{\Delta_1}, \mathcal{F}_{\Delta_2}$  respectively. Then, we have

$$I(X; Y) = \lim_{\Delta_1, \Delta_2 \rightarrow 0} I(X_{\Delta_1}, Y_{\Delta_2}).$$

*Proof:* We now use the general definition of mutual information given in [34],

$$I(X; Y) \triangleq \sup_{\mathcal{E}, \mathcal{F}} I(X; Y)(\mathcal{E}, \mathcal{F}),$$

with

$$I(X; Y)(\mathcal{E}, \mathcal{F}) \triangleq \sum_{i,j} \mathbb{P}_{XY}(E_i \times F_j) \log \frac{\mathbb{P}_{XY}(E_i \times F_j)}{\mathbb{P}_X(E_i) \mathbb{P}_Y(F_j)}.$$

Let  $\epsilon, \epsilon_1 > 0$ . Let  $\mathcal{E}_0 = \{E_i^0\}_{i \in \mathcal{I}_0}, \mathcal{F}_0 = \{F_j^0\}_{j \in \mathcal{J}_0}$  be partitions of  $X$  and  $Y$ , such that  $|I(X; Y)(\mathcal{E}_0, \mathcal{F}_0) - I(X; Y)| \leq \epsilon/2$ . Let  $\mathcal{E}_{\Delta_1} = \{E_i\}_{i \in \mathcal{I}}, \mathcal{F}_{\Delta_2} = \{F_j\}_{j \in \mathcal{J}}$  be partitions of  $X$  and  $Y$ , where  $\Delta_1, \Delta_2 > 0$ . Let  $\tilde{\mathcal{E}} = \{\tilde{E}_i^0\}_{i \in \mathcal{I}}, \tilde{\mathcal{F}} = \{\tilde{F}_j^0\}_{j \in \mathcal{J}}$  be partition of  $X$  and  $Y$  such that they have for sub-partition  $\mathcal{E}_{\Delta_1}, \mathcal{F}_{\Delta_2}$  respectively. Then, we choose  $\Delta_1, \Delta_2$  small enough such that for any  $i \in \mathcal{I}_0$ , for any  $j \in \mathcal{J}_0$ ,  $\mathbb{P}_X((E_i^0 \setminus \tilde{E}_i^0) \cup (\tilde{E}_i^0 \setminus E_i^0)) < \epsilon_1, \mathbb{P}_Y((F_j^0 \setminus \tilde{F}_j^0) \cup (\tilde{F}_j^0 \setminus F_j^0)) < \epsilon_1$ . Now by [33],

$$I(X_{\Delta_1}, Y_{\Delta_2}) = I(X; Y)(\mathcal{E}_{\Delta_1}, \mathcal{F}_{\Delta_2}) \geq I(X; Y)(\tilde{\mathcal{E}}, \tilde{\mathcal{F}}).$$

Then, for  $\epsilon_1$  small enough

$$I(X_{\Delta_1}, Y_{\Delta_2}) \geq I(X; Y)(\mathcal{E}_0, \mathcal{F}_0) - \epsilon/2.$$

Hence,

$$I(X; Y) \geq I(X_{\Delta_1}, Y_{\Delta_2}) \geq I(X; Y) - \epsilon.$$

■

Let  $\delta > 0$ . Let  $\Delta_1, \Delta_2 > 0$ . As in Lemma 3, from partitions of  $X, Y, U, V$ , and  $Z$ , we construct  $U_{\Delta_1}, V_{\Delta_1}, X_{\Delta_1}, Y_{\Delta_1}, Z_{\Delta_2}$ . Let us apply the proof of the discrete case to the random variables  $U_{\Delta_1}, V_{\Delta_1}, X_{\Delta_1}, Y_{\Delta_1}$ , and  $Z_{\Delta_2}$ . By Lemma 3 if we let  $\Delta_2 \rightarrow 0$ , then Equation (27) becomes

$$k = \lfloor N[I(U_{\Delta_1}; Y_{\Delta_1}) - I(V_{\Delta_1}; X_{\Delta_1}|U_{\Delta_1}) - I(U_{\Delta_1}; Z) - I(V_{\Delta_1}; Z|U_{\Delta_1})] - r_3(\epsilon, N) - \sqrt{N} \rfloor,$$

then, by Lemma 3 we choose  $\Delta_1$  such that  $|I(U_{\Delta_1}; Y_{\Delta_1}) - I(U; Y)| < \delta/4, |I(V_{\Delta_1}; X_{\Delta_1}|U_{\Delta_1}) - I(V; X|U)| < \delta/4, |I(U_{\Delta_1}; Z) - I(U; Z)| < \delta/4$ , and  $|I(V_{\Delta_1}; Z|U_{\Delta_1}) - I(V; Z|U)| < \delta/4$ . Hence,

$$k \geq \lfloor N[I(Y; U) - I(V; X|U) - I(U; Z) - I(V; Z|U)] - N\delta - r_3(\epsilon, N) - \sqrt{N} \rfloor. \quad (30)$$

At this point, we cannot conclude with the last inequality. Indeed, in the term  $r_3(\epsilon, N)$  are hidden the following terms:  $NH(X_{\Delta_1}|ZY_{\Delta_1}U_{\Delta_1})\epsilon$  (see (18)),  $NH(Y_{\Delta_1}|ZU_{\Delta_1}V_{\Delta_1})\epsilon$  (see (22)),  $NH(U_{\Delta_1})\epsilon$  and

$NH(V_{\Delta_1}|U_{\Delta_1})\epsilon$  (by definition of  $r_0(\epsilon)$ ), which do not go to 0 as  $N$  goes to infinity after normalization by  $N$ . Now, if we choose  $\epsilon = n^{-a}$ , where  $a \in ]0, 1/2[$ , so that for  $i \in \llbracket 0, 5 \rrbracket$ ,  $\delta_\epsilon^i(n) = \delta(N)$ ,<sup>18</sup> then

$$R = \frac{k}{N} = I(Y; U) - I(V; X|U) - I(U; Z) - I(V; Z|U) - \delta - \delta(N).$$

Moreover, we still have a leakage verifying (28), and Alice and Bob still share the same key  $K$  asymptotically, because in Equation (29),  $P_e(\epsilon, n)$  exponentially decreases with  $n$  with the previous choice of  $\epsilon$ .

### B. Proof of Theorem 5

Theorem 5 is not directly deduced from Theorem 4. We first consider the case of one-way public communication, in which Alice sends messages to Bob, a first time with rate  $R_1$  and a second time with rate  $R_2$ . For this scenario we note  $C_{\text{rec}}^*$  the reconciliation capacity.

We can modify the proof of Proposition 1 to obtain<sup>19</sup> the reconciliation capacity. For  $R_1, R_2 \in \mathbb{R}^+$ ,

$$C_{\text{rec}}^*(R_1, R_2) = \max_{U, V} [I(U; Y) + I(V; Y|U)] \text{ subject to}$$

$$R_1 \geq I(X; U|Y) \tag{31}$$

$$R_2 \geq I(V; X|YU) \tag{32}$$

$$U \rightarrow X \rightarrow Y, \tag{33}$$

$$V \rightarrow UX \rightarrow Y. \tag{34}$$

Then, we can modify the proof of Theorem 4 to prove that<sup>20</sup> we can achieve the rate

$$R_{\text{WSK}}^*(R_1, R_2) = \max_{U, V} ([I(Y; U) - I(Z; U)]^+ + [I(Y; V|U) - I(Z; V|U)]^+),$$

subject to rate constraints (31), (32) and Markov conditions (33), (34), by a reconciliation phase followed by a privacy amplification phase performed with extractors, and this time without the assumption  $X \rightarrow Y \rightarrow Z$ . Then, observe that

$$R_{\text{WSK}}^*(0, R_2) \geq \max_{U, V} [I(Y; V|U) - I(Z; V|U)],$$

<sup>18</sup>Recall that  $P_e(\epsilon, n)$  decreases exponentially to zero as  $n\epsilon^2$  goes to infinity.

<sup>19</sup>The proof can be found in Appendix G-A.

<sup>20</sup>The proof can be found in Appendix G-B.

subject to rate constraints  $I(U; X) - I(U; Y) = R_1 = 0$ , (32) and Markov conditions (33), (34). Note that Markov condition

$$U \rightarrow V \rightarrow X \rightarrow YZ, \quad (35)$$

implies Markov conditions (33) and (34) and that if Markov condition (35) holds, then the rate constraint (32) becomes

$$R_2 \geq I(X; V|U) - I(Y; V|U) = I(X; V) - I(Y; V) - I(X; U) + I(Y; U),$$

so that

$$R_{\text{WSK}}^*(0, R_2) \geq \max_{U, V} [I(X; V|U) - I(Z; V|U)],$$

subject to rate constraint  $R_2 \geq I(X; V) - I(Y; V)$  and Markov condition (35). Hence,  $R_{\text{WSK}}^*(0, R_2) \geq C_{\text{WSK}}(R_2, 0)$  by Theorem 1.b.

### C. Proof of Theorem 6

The proof of Theorem 6 is the same as the one of Theorem 4 without the RV  $Z$ . We are able to show that reconciliation and privacy amplification can be treated independently because by Proposition 1, for  $R_1, R_2 \in \mathbb{R}^+$ ,

$$C_{\text{rec}}(R_1, R_2) = C_{\text{SK}}(R_1, R_2),$$

which means that the auxiliary RVs  $(U, V)$  (resp.  $U$ ) maximizing  $C_{\text{rec}}(R_1, R_2)$  in Theorem 1 and  $C_{\text{WSK}}(R_1, R_2)$  in Corollary 2.2 (resp.  $C_{\text{rec}}(R_1, 0)$  in Theorem 1 and  $C_{\text{WSK}}(R_1, 0)$  in Corollary 2.b) are the same. Hence, an optimal reconciliation leads to an optimal sequential key-distillation.

## APPENDIX C

### PROOF OF PROPOSITION 2

The proof is partially found in [16] and all that remains to be proved are the equality in the communication rate constraint and the range constraint  $|\mathcal{U}| \leq |\mathcal{X}|$ .

#### A. Equality in the constraint

To prove that equality holds in the constraint for the argument of the maximum in Proposition 2, we can reuse the proof of Proposition 1 in Appendix A-A, so that we only need to show that  $f(U) = I(Y; U) - I(Z; U)$  is convex in  $p_{U|X}$ . To obtain the convexity of  $f$ , we replace  $(X, Y)$  by  $(Y, Z)$  in the function  $f_1$  of Lemma 1.

### B. Range constraint $|\mathcal{U}| \leq |\mathcal{X}|$

The proof relies on a technique used in [36].

Define  $\mathcal{R} \triangleq \{(R, R_1) : R \geq I(Y; U) - I(Z; U), R_1 \geq I(X; U) - I(Y; U), \text{ with } U \rightarrow X \rightarrow Y\}$ , and  $\mathcal{C} \triangleq \{(R, R_1) : R \geq I(Y; U) - I(Z; U), R_1 = I(X; U) - I(Y; U), \text{ with } U \rightarrow X \rightarrow Y\}$ .

Note that the capacity region  $\mathcal{C}$  is from Proposition 2 and that the equality in the communication rate constraint is crucial to make it a subset of  $\mathcal{R}$ . By [36, Lemma 3],

$$\mathcal{R} = \{(R, R_1) : \forall \lambda_1, \lambda_2 \in \mathbb{R}^+, \lambda_1 R + \lambda_2 R_1 \geq G(\lambda_1, \lambda_2)\},$$

where  $\forall \lambda_1, \lambda_2 \in \mathbb{R}^+$ ,  $G(\lambda_1, \lambda_2) \triangleq \inf_{U \text{ s.t. } U \rightarrow X \rightarrow Y} [\lambda_1(I(Y; U) - I(Z; U)) + \lambda_2(I(X; U) - I(Y; U))]$ .

Consequently  $G(\lambda_1, \lambda_2)$  is sufficient information to describe  $\mathcal{R}$ . Then, we show that for all  $\lambda_1, \lambda_2 \in \mathbb{R}^+$ ,  $G(\lambda_1, \lambda_2)$  can be achieved by considering a discrete random variable  $U$  such that  $|\mathcal{U}| \leq |\mathcal{X}|$ .

Let  $\lambda_1, \lambda_2 \in \mathbb{R}^+$ , let  $\mathcal{P}$  in [36, Lemma 2] be the  $|\mathcal{X}|$ -dimensional probability simplex, and let  $\mathcal{X} = \{x_i\}_{i=1}^{|\mathcal{X}|}$ . Consider  $\mathcal{P}$  as a set of elements of the form of  $P$ , where

$$P = (\mathbb{P}(X = x_1|U = u), \mathbb{P}(X = x_2|U = u), \dots, \mathbb{P}(X = x_{|\mathcal{X}|}|U = u)),$$

with  $u \in \mathcal{U}$ . Then, each probability distribution on  $U$  defines a measure  $\mu$  on  $\mathcal{P}$ . Define  $H_P(X)$ ,  $H_P(Y)$ , and  $H_P(Z)$  as the entropies of  $X$ ,  $Y$ , and  $Z$  respectively, when the distribution of  $X$  is  $P$ . Define

$$f_1(P) \triangleq \lambda_1(H_P(Z) - H_P(Y)) + \lambda_2(H_P(Y) - H_P(X))$$

$$f_j(P) \triangleq P(x_j), \text{ for } j \in \llbracket 2, |\mathcal{X}| \rrbracket.$$

Let  $P_X^*$  achieve  $G(\lambda_1, \lambda_2)$ , and let  $\mu^*$  be such that  $\int_{\mathcal{P}} P \mu^*(dP) = P_X^*$ . Denote by  $H^*(X)$  the entropy of  $X$  under probability distribution  $P_X^*$ . Then, by [36, Lemma 2], there exists  $P_1, P_2, \dots, P_{|\mathcal{X}|}$ , and  $\alpha_1, \alpha_2, \dots, \alpha_{|\mathcal{X}|}$  such that,  $\sum_{i=1}^{|\mathcal{X}|} \alpha_i = 1$ , for  $j \in \llbracket 2, |\mathcal{X}| \rrbracket$

$$P_X^*(x_j) = \int_{\mathcal{P}} f_j(P) \mu^*(dP) = \sum_{i=1}^{|\mathcal{X}|} \alpha_i f_j(P_i),$$

and,

$$\begin{aligned} & \lambda_1(H^*(Z|U) - H^*(Y|U)) + \lambda_2(H^*(Y|U) - H^*(X|U)) \\ &= \lambda_1 \int_{\mathcal{P}} (H_P(Z) - H_P(Y)) \mu^*(dP) + \lambda_2 \int_{\mathcal{P}} (H_P(Y) - H_P(X)) \mu^*(dP) \\ &= \int_{\mathcal{P}} f_1(P) \mu^*(dP) \\ &= \sum_{i=1}^{|\mathcal{X}|} \alpha_i f_1(P_i). \end{aligned}$$



From  $P_X^*(x_j)$ ,  $j \in \llbracket 2, |\mathcal{X}| \rrbracket$ , we can compute  $H^*(X)$ ,  $H^*(Y)$ , and  $H_P(Z)$ , since  $U \rightarrow X \rightarrow Y \rightarrow Z$ . Hence,

$$\begin{aligned} & \lambda_1(H^*(Y) - H^*(Y|U) - H^*(Z) + H^*(Z|U)) + \lambda_2(H^*(X) - H^*(X|U) - H^*(Y) + H^*(Y|U)) \\ &= \lambda_1(I^*(Y; U) - I^*(Z; U)) + \lambda_2(I^*(X; U) - I^*(Y; U)) \\ &= G(\lambda_1, \lambda_2). \end{aligned}$$

We have thus shown that we can choose  $U$  such that  $|\mathcal{U}| \leq |\mathcal{X}|$  to achieve  $G(\lambda_1, \lambda_2)$ . Consequently, it is enough to consider  $U$  such that  $|\mathcal{U}| \leq |\mathcal{X}|$ , to form the set  $\mathcal{R}$ , as well as the set  $\mathcal{C}$ , since  $\mathcal{C} \subset \mathcal{R}$ .

#### APPENDIX D

##### PROOF OF PROPOSITION 3

If  $R_1 \geq H(X|Y)$ , then by Proposition 2  $C_{\text{WSK}}(R_1, 0) = \mathbb{I}(X; Y)$ . Assume  $R_1 \in ]0; H(X|Y[$  in the following. We note  $\mathcal{X} = \{0, 1\}$  and by Proposition 2, we can assume  $\mathcal{U} = \{u_1, u_2\}$ . We note  $\beta_1 = p(X = 1|U = u_1)$  and  $\beta_2 = p(X = 0|U = u_2)$ . We can write

$$\begin{aligned} I(U; X) - I(U; Y) &= H(X) - H(Y) - \sum_{i=1,2} p(u_i)[H(X|U = u_i) - H(Y|U = u_i)] \\ &= 1 - H(Y) - \sum_{i=1,2} p(u_i)[H_b(\beta_i) - H(Y|U = u_i)] \\ &= 1 - H(Y) - \sum_{i=1,2} p(u_i) \left[ H_b(\beta_i) + \sum_{y \in \mathcal{Y}} p(y|u_i) \log p(y|u_i) \right], \end{aligned} \quad (36)$$

with  $\forall y \in \mathcal{Y}$ ,

$$p(y|u_1) = \sum_{x \in \mathcal{X}} p(x|u_1)p(y|x) = (1 - \beta_1)p(y|x = 0) + \beta_1 p(y|x = 1), \quad (37)$$

$$p(y|u_2) = \sum_{x \in \mathcal{X}} p(x|u_2)p(y|x) = \beta_2 p(y|x = 0) + (1 - \beta_2)p(y|x = 1). \quad (38)$$

Moreover, since the channel  $p_{Y|X}$  is symmetric, there exists a permutation  $\pi \in \mathfrak{S}_{|\mathcal{Y}|}$  such that

$$\forall y \in \mathcal{Y}, \forall x \in \mathcal{X}, p(y|x) = p(\pi(y)|x \oplus 1), \quad (39)$$

where  $\oplus$  denotes the modulo 2 operation. Thus by (37), (38), (39) there exists  $g_{Y|X}$ <sup>21</sup> such that  $H(Y|U = u_1) = g_{Y|X}(\beta_1)$ ,  $H(Y|U = u_2) = g_{Y|X}(\beta_2)$ . Then,

$$I(U; X) - I(U; Y) = 1 - H(Y) - \sum_{i=1,2} p(u_i) [H_b(\beta_i) - g_{Y|X}(\beta_i)]. \quad (40)$$

Similarly, by using that the channel  $p_{Z|X}$  is symmetric, there exists  $g_{Z|X}$  such that  $H(Z|U = u_1) = g_{Z|X}(\beta_1)$  and  $H(Z|U = u_2) = g_{Z|X}(\beta_2)$ . Thus, we also have

$$I(U; Y) - I(U; Z) = H(Y) - H(Z) - \sum_{i=1,2} p(u_i) [g_{Y|X}(\beta_i) - g_{Z|X}(\beta_i)]. \quad (41)$$

Consider the region  $\mathcal{R}_1$  and  $\mathcal{R}_2$

$$\mathcal{R}_1 \triangleq \{(R, R_1) | R \leq H(Y) - H(Z) - g_{Y|X}(\beta_0) + g_{Z|X}(\beta_0),$$

$$R_1 \leq 1 - H(Y) - H_b(\beta_0) + g_{Y|X}(\beta_0), \beta_0 \in [0, 1]\},$$

$$\mathcal{R}_2 \triangleq \{(R, R_1) | R \leq I(Y; U) - I(Z; U), R_1 \leq I(X; U) - I(Y; U), (\beta_1, \beta_2) \in [0, 1]^2\}.$$

We easily verify that both regions  $\mathcal{R}_1$  and  $\mathcal{R}_2$  are convex and that  $\mathcal{R}_1 \subset \mathcal{R}_2$ . We will use a similar technique as in [37], based on Lemma 4, to show that  $\mathcal{R}_1 = \mathcal{R}_2$ . Then, thanks to the refinement proposed in Proposition 2 (equality in the constraint), we will be able to conclude

$$\begin{aligned} & \{(R, R_1) | R \leq H(Y) - H(Z) - g_{Y|X}(\beta_0) + g_{Z|X}(\beta_0), R_1 = 1 - H(Y) - H_b(\beta_0) + g_{Y|X}(\beta_0), \beta_0 \in [0, 1]\} \\ &= \{(R, R_1) | R \leq I(Y; U) - I(Z; U), R_1 = I(X; U) - I(Y; U), (\beta_1, \beta_2) \in [0, 1]^2\}. \end{aligned}$$

**Lemma 4** ([37] [25]). *Let  $\mathcal{C} \subset \mathbb{R}^d$  be convex. Let  $\mathcal{C}_1 \subset \mathcal{C}_2$  be two bounded convex subsets of  $\mathcal{C}$ , closed relative to  $\mathcal{C}$ . If every supporting hyperplanes of  $\mathcal{C}_2$  intersects with  $\mathcal{C}_1$ , then  $\mathcal{C}_1 = \mathcal{C}_2$ .*

Let  $(R, R_1) \in \mathcal{R}_2$ , and let  $\alpha \in [0, 1]$ , then we have by (40), (41)

$$\begin{aligned} & \alpha R + (1 - \alpha)R_1 \\ & \leq \alpha(I(Y; U) - I(Z; U)) + (1 - \alpha)(I(X; U) - I(Y; U)) \\ &= \sum_{i=1,2} [\alpha(H(Y) - H(Z) - g_{Y|X}(\beta_i) + g_{Z|X}(\beta_i)) + (1 - \alpha)(1 - H(Y) - H_b(\beta_i) + g_{Y|X}(\beta_i))]p(u_i) \\ & \leq \alpha(H(Y) - H(Z) - g_{Y|X}(\beta^*) + g_{Z|X}(\beta^*)) + (1 - \alpha)(1 - H(Y) - H_b(\beta^*) + g_{Y|X}(\beta^*)), \quad (42) \end{aligned}$$

<sup>21</sup>The exact description of  $g_{Y|X}$  is not important here, what matters is that  $H(Y|U = u_1)$  and  $H(Y|U = u_2)$  can be expressed with the same function.

where  $\beta^* = \operatorname{argmax}_{\beta}(\alpha(H(Y) - H(Z) - g_{Y|X}(\beta) + g_{Z|X}(\beta)) + (1 - \alpha)(1 - H(Y) - H_b(\beta) + g_{Y|X}(\beta)))$ .

With the last inequality, we show that every supporting plane of  $\mathcal{R}_2$  intersects  $\mathcal{R}_1$ . Note that the weight coefficients of  $(R, R_1)$  have been taken of the form  $(\alpha, 1 - \alpha)$  with  $\alpha \in [0, 1]$ , because by positivity and convexity of  $\mathcal{R}_2$ , we only needed to consider hyperplanes (lines) with negative slope to apply Lemma 4. Let  $(R^0, R_1^0)$  be a boundary point of  $\mathcal{R}_2$ . There exists a supporting hyperplane  $\mathcal{H}_0$  at  $(R^0, R_1^0)$  defined by  $(\alpha^0, 1 - \alpha^0)$ . By equation (42), there exists  $\beta_0^* \in [0, 1]$  such that

$$\alpha^0 R^0 + (1 - \alpha^0) R_1^0 \leq \alpha^0 R^* + (1 - \alpha^0) R_1^*,$$

where  $(R^*, R_1^*) \triangleq (H(Y) - H(Z) - g_{Y|X}(\beta^*) + g_{Z|X}(\beta^*), 1 - H(Y) - H_b(\beta^*) + g_{Y|X}(\beta^*))$ . Then, since  $(R^*, R_1^*) \in \mathcal{R}_1 \subset \mathcal{R}_2$ , we also have, by definition of  $\mathcal{H}_0$

$$\alpha^0 R^* + (1 - \alpha^0) R_1^* \leq \alpha^0 R^0 + (1 - \alpha^0) R_1^0.$$

Hence,  $\alpha^0 R^* + (1 - \alpha^0) R_1^* = \alpha^0 R^0 + (1 - \alpha^0) R_1^0$ , and thus  $(R^*, R_1^*) \in \mathcal{H}_0$ .

## APPENDIX E

### PROOF OF PROPOSITION 6

Consider  $X \sim \mathcal{N}(0, \sigma_x^2)$ ,  $N \sim \mathcal{N}(0, \sigma_n^2)$ ,  $Y = X + N$ . We have  $\sigma_y^2 = \sigma_x^2 + \sigma_n^2$  and

$$p_X(x) = \frac{1}{\sqrt{2\pi\sigma_x^2}} \exp\left[-\frac{x^2}{2\sigma_x^2}\right], \quad p_{X|Y}(x|y) = \frac{1}{\sqrt{2\pi}} \frac{\sigma_y}{\sigma_x \sigma_n} \exp\left[-\frac{1}{2\sigma_n^2} \frac{\sigma_y^2}{\sigma_x^2} \left(x - \frac{\sigma_x^2}{\sigma_y^2} y\right)^2\right].$$

Let  $n \in \mathbb{Z}$ . Let  $\Delta > 0$ . Define  $U$ , a scalar quantized version of  $X$ , as follows:

$$p_{U|Y}(u_n|y) = p_{X|Y}(t_n|y)\Delta, \quad p_U(u_n) = p_X(t_n)\Delta, \quad \text{where } t_n = \Delta/2 + (n - 1)\Delta.$$

Then,

$$H(U) = -\sum_n p_U(u_n) \log p_U(u_n) = S_U - \log \Delta, \quad \text{where } S_U \triangleq -\sum_n \Delta p_X(t_n) \log p_X(t_n).$$

Observe that  $S_U$  is a middle Riemann sum that approaches  $h(X) = -\int p_X(x) \log p_X(x) dx$ . Thus, if we set  $f(x) \triangleq -p_X(x) \log p_X(x)$ , we can show that for any  $a \in \mathbb{R}^+$ ,<sup>22</sup>

$$\begin{aligned} |h(X) - S_U| &= \left| \int f - S_U \right| \\ &\leq \left| \int_{-\infty}^{-a} + \int_a^{+\infty} f(x) dx \right| + \left| S_U - \int_{-a}^a f(x) dx \right| \\ &\leq \epsilon_1(a) + K_1(a) \Delta^2, \end{aligned}$$

<sup>22</sup>We used the middle Riemann sum error bound, and  $\operatorname{erfc}(x) \leq e^{-x^2}$ .

with  $K_1(a) = \frac{a}{12} \max_{[-a,a]} |f''|$ ,  $\epsilon_1(a) = e^{-\frac{a^2}{2\sigma_x^2}} [\alpha_1 a + \beta_1]$ , where  $\alpha_1 = \frac{1}{\sqrt{2\pi}\sigma_x}$ ,  $\beta_1 = \left| \log \frac{1}{\sqrt{2\pi}\sigma_x} - \frac{1}{2} \right|$ .

Similarly, if we define

$$S_{U|Y} \triangleq - \sum_n \Delta \int_y p_Y(y) p_{X|Y}(t_n|y) \log p_{X|Y}(t_n|y) dy, \text{ and } g(x) \triangleq \int_y p_Y(y) p_{X|Y}(x|y) \log p_{X|Y}(x|y) dy,$$

then, as previously, we can show that for any  $a \in \mathbb{R}^+$ ,

$$|h(X|Y) - S_{U|Y}| \leq \epsilon_2(a) + K_2(a)\Delta^2,$$

$$\text{with } K_2(a) = \frac{a}{12} \max_{[-a,a]} |g''|, \epsilon_2(a) = e^{-\frac{a^2}{2\sigma_x^2}} [\alpha_2 a + \beta_2], \text{ where } \alpha_2 = \frac{1}{\sqrt{2\pi}} \frac{(\sigma_y^2 - \frac{\sigma_x^2}{\sqrt{2\sigma_n^2}})^2}{\sigma_y^2 \sigma_n^3},$$

$$\beta_2 = \frac{\sqrt{\pi}}{2} \alpha_2 + \left| \frac{1}{2\sqrt{2}\sigma_n} \left( \frac{1}{2\sigma_n^2} \frac{\sigma_x^2}{\sigma_y^2} - \log \left( \frac{1}{2\pi\sigma_n^2} \frac{\sigma_y^2}{\sigma_x^2} \right) \right) \right|.$$

Thus,

$$\log \Delta - (\epsilon_2(a) + K_2(a)\Delta^2) \leq h(X|Y) - H(U|Y) \leq \log \Delta + \epsilon_2(a) + K_2(a)\Delta^2.$$

Hence, for any  $a \in \mathbb{R}^+$ , if we take  $\Delta$  small enough, then  $\log \Delta \gg \epsilon_2(a) + K_2(a)\Delta^2$ , such that  $h(X|Y) - H(U|Y) \approx \log \Delta$ , and

$$\begin{aligned} |I(X;Y) - I(Y;U)| &= |h(X) - S_U + S_{U|Y} - h(X|Y)| \\ &\leq \epsilon(a) + K(a)\Delta^2 \\ &\leq \epsilon(a) + K(a) \exp[2(h(X|Y) - H(U|Y))] \\ &= \epsilon(a) + K(a) \exp[2(h(X|Y) - R_1)], \end{aligned} \tag{43}$$

where  $\epsilon(a) = \epsilon_1(a) + \epsilon_2(a)$ ,  $K(a) = K_1(a) + K_2(a)$ .

If we take  $a = \sigma_x \sqrt{2R_1}$  in (43), we obtain

$$|I(X;Y) - I(Y;U)| \leq [\alpha R_1 + \beta] e^{-R_1} + K \sqrt{R_1} e^{[2(h(X|Y) - R_1)]},$$

where  $\alpha = \alpha_1 + \alpha_2$ ,  $\beta = \beta_1 + \beta_2$ ,  $K = \frac{\sqrt{2}\sigma_x}{12} [\max(|f''| + |g''|)]$ . We can show that  $K \leq [|\log(\sqrt{2\pi}\sigma_x)| + 11 + 4\beta_2 + \sqrt{\pi}\alpha_2(11/\sqrt{2\sigma_n^2} - 2)]/[24\sqrt{\pi}\sigma_x^2]$ . To sum up, if  $R_1$  is large enough, i.e  $R_1 > h(X|Y)$ , then  $\Delta$  can be chosen small enough to ensure  $\log \Delta \gg \epsilon_2 + K_2\Delta^2$ , so that  $I(Y;U)$  approaches  $I(X;Y)$  exponentially fast as  $R_1$  increases.

## APPENDIX F

### ERROR ANALYSIS OF THE RECONCILIATION PROTOCOL

In this section, we detail the error probability analysis for the reconciliation capacity in Proposition 1. Although, the proof uses standard tools and is close to the work in [28], [10], we perform a finer analysis,

and show the exponential decrease of  $P_e(\epsilon, n)$  to zero as  $n\epsilon^2$  goes to infinity, which then allows us to extend our result to the case of a continuous source model.

In the following, we use the same notations as in Appendix A-B2. Define,

$$\forall(\omega, \nu, k, l) \in \llbracket 1, 2^{nR_u} \rrbracket \times \llbracket 1, 2^{nR'_u} \rrbracket \times \llbracket 1, 2^{nR_v} \rrbracket \times \llbracket 1, 2^{nR'_v} \rrbracket,$$

$$\mathcal{A}_0 \triangleq \{(X^n, Y^n) \notin \mathcal{T}_{\epsilon_1}^n(XY)\},$$

$$\mathcal{E}_{\omega, \nu} \triangleq \{(u^n(\omega, \nu), X^n) \notin \mathcal{T}_{\epsilon}^n(UX)\},$$

$$\mathcal{F}_{\omega, \nu} \triangleq \{(u^n(\omega, \nu), Y^n) \notin \mathcal{T}_{\epsilon}^n(UY)\},$$

$$\mathcal{G}_{\omega, \nu, k, l} \triangleq \{(u^n(\omega, \nu), Y^n, v^n(\omega, \nu, k, l)) \notin \mathcal{T}_{\epsilon_2}^n(UYV)\},$$

$$\mathcal{H}_{\omega, \nu, k, l} \triangleq \{(u^n(\omega, \nu), X^n, v^n(\omega, \nu, k, l)) \notin \mathcal{T}_{\epsilon_2}^n(UXV)\}.$$

Define

$$\begin{aligned} \mathcal{A}_1 &\triangleq \left\{ \bigcap_{\omega} \bigcap_{\nu} \mathcal{E}_{\omega, \nu} \right\}, \\ \mathcal{A}_2 &\triangleq \left\{ \bigcup_{\bar{\nu} \neq N} \mathcal{F}_{\Omega, \bar{\nu}}^c \right\}, \\ \mathcal{A}_3 &\triangleq \left\{ \bigcap_{\bar{\nu}} \mathcal{F}_{\Omega, \bar{\nu}} \right\}, \\ \mathcal{A}_4 &\triangleq \left\{ \bigcap_k \bigcap_l \mathcal{G}_{\Omega, N, k, l} \right\}, \\ \mathcal{A}_5 &\triangleq \left\{ \bigcup_{\bar{l} \neq L} \mathcal{H}_{\Omega, N, K, \bar{l}}^c \right\}, \\ \mathcal{A}_6 &\triangleq \left\{ \bigcap_{\bar{l}} \mathcal{H}_{\Omega, N, K, \bar{l}} \right\}, \end{aligned}$$

where indices with capital letters denote random variables.

We have

$$\begin{aligned}
P_e(\epsilon, n, \mathcal{C}_n) &= \mathbb{P} \left[ \bigcup_{i=1}^6 \mathcal{A}_i \right] \\
&\leq \mathbb{P} \left[ \bigcup_{i=0}^6 \mathcal{A}_i \right] \\
&\leq \mathbb{P} \left[ \bigcup_{i=0}^6 \mathcal{A}_i \cap \mathcal{A}_0^c \right] + \mathbb{P}[\mathcal{A}_0] \\
&= \sum_{i=1}^6 \mathbb{P} \left[ \mathcal{A}_i \cap \bigcap_{j=0}^{i-1} \mathcal{A}_j^c \right] + \mathbb{P}[\mathcal{A}_0] \\
&= \sum_{i=0}^6 P_{e_i},
\end{aligned}$$

where  $P_{e_i} \triangleq \mathbb{P} \left[ \mathcal{A}_i \cap \bigcap_{j=0}^{i-1} \mathcal{A}_j^c \right]$ , for  $i = \llbracket 1, 6 \rrbracket$  and  $P_{e_0} \triangleq \mathbb{P}[\mathcal{A}_0]$ . We now upper-bound  $\mathbb{E}_{C_n}[P_{e_i}]$  for  $i \in \llbracket 0, 6 \rrbracket$  by using the tools in [30].

$$\mathbb{E}_{C_n}[P_{e_0}] = 2|\mathcal{X}||\mathcal{Y}|\exp(-n\epsilon_1^2\mu_{XY}),$$

$$\begin{aligned}
\mathbb{E}_{C_n}[P_{e_1}] &= \mathbb{E}_{C_n} \left[ \sum_{x^n, y^n} p(x^n, y^n) \mathbf{1} \left\{ \forall (\omega, \nu), (u^n(\omega, \nu), x^n) \notin \mathcal{T}_\epsilon^n(UX) \text{ and } (x^n, y^n) \in \mathcal{T}_{\epsilon_1}^n(XY) \right\} \right] \\
&= \mathbb{E}_{C_n} \left[ \sum_{(x^n, y^n) \in \mathcal{T}_{\epsilon_1}^n(XY)} p(x^n, y^n) \mathbf{1} \left\{ \forall (\omega, \nu), (u^n(\omega, \nu), x^n) \notin \mathcal{T}_\epsilon^n(UX) \right\} \right] \\
&= \sum_{(x^n, y^n) \in \mathcal{T}_{\epsilon_1}^n(XY)} p(x^n, y^n) \mathbb{P} \left\{ \forall (\omega, \nu), (U^n(\omega, \nu), x^n) \notin \mathcal{T}_\epsilon^n(UX) \right\} \\
&= \sum_{(x^n, y^n) \in \mathcal{T}_{\epsilon_1}^n(XY)} p(x^n, y^n) (1 - \mathbb{P}[(U^n(\omega, \nu), x^n) \in \mathcal{T}_\epsilon^n(UX)])^{2^{n(R_u + R'_u)}} \\
&\leq \sum_{(x^n, y^n) \in \mathcal{T}_{\epsilon_1}^n(XY)} p(x^n, y^n) \exp \left( -2^{n(R_u + R'_u)} \mathbb{P}[(U^n(\omega, \nu), x^n) \in \mathcal{T}_\epsilon^n(UX)] \right) \\
&\leq \sum_{(x^n, y^n) \in \mathcal{T}_{\epsilon_1}^n(XY)} p(x^n, y^n) \exp \left( -2^{n(R_u + R'_u)} \left( 1 - \delta_{\epsilon_1, \epsilon}^{(1)}(n) \right) 2^{-n(I(U; X) + 2\epsilon H(U))} \right) \\
&\leq \exp \left( - \left( 1 - \delta_{\epsilon_1, \epsilon}^{(1)}(n) \right) 2^{n(R_u + R'_u - I(U; X) - 2\epsilon H(U))} \right) \\
&= \exp \left( - \left( 1 - \delta_{\epsilon_1, \epsilon}^{(1)}(n) \right) 2^{\epsilon H(U)} \right),
\end{aligned}$$

where  $\delta_{\epsilon_1, \epsilon}^{(1)}(n) \triangleq 2|\mathcal{X}||\mathcal{U}|\exp \left( -n \frac{(\epsilon - \epsilon_1)^2}{1 + \epsilon_1} \mu_{UY} \right)$ ,

$$\begin{aligned}
& \mathbb{E}_{C_n}[P_{e_2}] \\
& \leq \sum_{\omega, \nu} p(\omega, \nu) \sum_{\bar{\nu} \neq \nu} \mathbb{E}_{C_n} \left[ \sum_{(x^n, y^n) \in \mathcal{T}_{\epsilon_1}^n(XY)} p(x^n, y^n) \mathbb{1}\{(y^n, u^n(\omega, \bar{\nu})) \in \mathcal{T}_{\epsilon}^n(YU) \text{ and } (x^n, u^n(\omega, \nu)) \in \mathcal{T}_{\epsilon}^n(XU)\} \right] \\
& \leq \sum_{\omega, \nu} p(\omega, \nu) \sum_{\bar{\nu} \neq \nu} \mathbb{E}_{C_n} \left[ \sum_{(x^n, y^n) \in \mathcal{T}_{\epsilon_1}^n(XY)} p(x^n, y^n) \mathbb{1}\{(y^n, u^n(\omega, \bar{\nu})) \in \mathcal{T}_{\epsilon}^n(YU)\} \right] \\
& = \sum_{\omega, \nu} p(\omega, \nu) \sum_{\bar{\nu} \neq \nu} \sum_{(x^n, y^n) \in \mathcal{T}_{\epsilon_1}^n(XY)} p(x^n, y^n) \mathbb{P}[(y^n, U^n(\omega, \bar{\nu})) \in \mathcal{T}_{\epsilon}^n(YU)] \\
& \leq \sum_{\omega, \nu} p(\omega, \nu) \sum_{\bar{\nu} \neq \nu} \sum_{(x^n, y^n) \in \mathcal{T}_{\epsilon_1}^n(XY)} p(x^n, y^n) 2^{-n(I(U; Y) - 2\epsilon H(U))} \\
& \leq 2^{n(R'_u - I(U; Y) + 2\epsilon H(U))} \\
& = 2^{-n\epsilon H(U)},
\end{aligned}$$

$$\begin{aligned}
& \mathbb{E}_{C_n}[P_{e_3}] \\
& \leq \sum_{\omega, \nu} p(\omega, \nu) \sum_{(x^n, y^n) \in \mathcal{T}_{\epsilon_1}^n(XY)} p(x^n, y^n) \mathbb{E}_{C_n} [\mathbb{1}\{\forall \bar{\nu}, (y^n, u^n(\omega, \bar{\nu})) \notin \mathcal{T}_{\epsilon}^n(YU)\}] \\
& \leq \sum_{\omega, \nu} p(\omega, \nu) \sum_{(x^n, y^n) \in \mathcal{T}_{\epsilon_1}^n(XY)} p(x^n, y^n) (\mathbb{P}[(y^n, U^n(\omega, \bar{\nu})) \notin \mathcal{T}_{\epsilon}^n(YU)])^{2^{nR'_u}} \\
& \leq (\delta_{\epsilon_1, \epsilon}^{(2)})^{2^{nR'_u}},
\end{aligned}$$

where  $\delta_{\epsilon_1, \epsilon}^{(2)} \triangleq 2|\mathcal{X}||\mathcal{Y}||\mathcal{U}| \exp\left(-n \frac{(\epsilon - \epsilon_1)^2}{1 + \epsilon_1} \mu_{XYZ}\right)$ ,

$$\begin{aligned}
& \mathbb{E}_{C_n}[P_{e_4}] \\
& \leq \sum_{\omega, \nu} p(\omega, \nu) \sum_{(x^n, y^n) \in \mathcal{T}_{\epsilon_1}^n(XY)} p(x^n, y^n) \\
& \quad \mathbb{E}_{C_n} [\mathbb{1}\{\forall(k, l), (u^n(\omega, \nu), y^n, v^n(\omega, \nu, k, l)) \notin \mathcal{T}_{\epsilon_2}^n(UYV) \text{ and } (y^n, u^n(\omega, \nu)) \in \mathcal{T}_{\epsilon}^n(YU)\}] \\
& \leq \sum_{\omega, \nu} p(\omega, \nu) \sum_{(x^n, y^n) \in \mathcal{T}_{\epsilon_1}^n(XY)} p(x^n, y^n) \\
& \quad \left( \sum_{u^n, v^n} p(u^n, v^n) \mathbb{P} [u^n(\omega, \nu), y^n, v^n(\omega, \nu, k, l)) \notin \mathcal{T}_{\epsilon_2}^n(UYV) \text{ and } (y^n, u^n(\omega, \nu)) \in \mathcal{T}_{\epsilon}^n(YU)] \right)^{2^{n(R_v + R'_v)}} \\
& \leq \sum_{\omega, \nu} p(\omega, \nu) \sum_{(x^n, y^n) \in \mathcal{T}_{\epsilon_1}^n(XY)} p(x^n, y^n) \left( 1 - \sum_{u^n: (u^n, y^n) \in \mathcal{T}_{\epsilon}^n(UY)} p(u^n) \sum_{v^n \in \mathcal{T}_{\epsilon_2}^n(VUY|u^n, y^n)} p(v^n|u^n) \right)^{2^{n(R_v + R'_v)}} \\
& \leq \sum_{\omega, \nu} p(\omega, \nu) \sum_{(x^n, y^n) \in \mathcal{T}_{\epsilon_1}^n(XY)} p(x^n, y^n) \\
& \quad \left( 1 - (1 - \delta_{\epsilon}^{(3)}(n))(1 - \delta_{\epsilon, \epsilon_2}^{(4)}(n)) 2^{nH(V|YU)(1-\epsilon_2)} 2^{-nH(V|U)(1+\epsilon_2)} \right)^{2^{n(R_v + R'_v)}} \\
& \leq \exp \left( -(1 - \delta_{\epsilon}^{(3)}(n))(1 - \delta_{\epsilon, \epsilon_2}^{(4)}(n)) 2^{n(R_v + R'_v + H(V|YU)(1-\epsilon_2) - nH(V|U)(1+\epsilon_2))} \right) \\
& = \exp \left( -(1 - \delta_{\epsilon}^{(3)}(n))(1 - \delta_{\epsilon, \epsilon_2}^{(4)}(n)) 2^{n(\epsilon_2(2H(V|U) - H(V|YU)))} \right), \\
& \text{where } \delta_{\epsilon}^{(3)}(n) \triangleq 2|\mathcal{X}||\mathcal{U}| \exp(-n\epsilon^2 \mu_{XU}), \delta_{\epsilon, \epsilon_2}^{(4)}(n) \triangleq 2|\mathcal{V}||\mathcal{Y}||\mathcal{U}| \exp \left( -n \frac{(\epsilon_2 - \epsilon)^2}{1 + \epsilon} \mu_{VYU} \right),
\end{aligned}$$

$$\begin{aligned}
& \mathbb{E}_{C_n}[P_{e_5}] \\
& \leq \sum_{\omega, \nu, k, l} p(\omega, \nu, k, l) \sum_{\bar{l} \neq l} \sum_{(x^n, y^n) \in \mathcal{T}_{\epsilon_1}^n(XY)} p(x^n, y^n) \\
& \quad \mathbb{E}_{C_n} [\mathbb{1}\{(x^n, u^n(\omega, \nu), v^n(\omega, \nu, k, \bar{l})) \in \mathcal{T}_{\epsilon_2}^n(XUV) \text{ and } (x^n, u^n(\omega, \nu)) \in \mathcal{T}_{\epsilon}^n(XU)\}] \\
& \leq \sum_{\omega, \nu, k, l} p(\omega, \nu, k, l) \sum_{\bar{l} \neq l} \sum_{(x^n, y^n) \in \mathcal{T}_{\epsilon_1}^n(XY)} p(x^n, y^n) \sum_{u^n: (u^n, x^n) \in \mathcal{T}_{\epsilon}^n(UX)} p(u^n) \sum_{v^n \in \mathcal{T}_{\epsilon_2}^n(VUX|u^n, x^n)} p(v^n|u^n) \\
& \leq \sum_{\omega, \nu, k, l} p(\omega, \nu, k, l) \sum_{\bar{l} \neq l} \sum_{(x^n, y^n) \in \mathcal{T}_{\epsilon_1}^n(XY)} p(x^n, y^n) \sum_{u^n: (u^n, x^n) \in \mathcal{T}_{\epsilon}^n(UX)} p(u^n) 2^{nH(V|UX)(1+\epsilon_2)} 2^{-nH(V|U)(1-\epsilon_2)} \\
& \leq 2^{n((H(V|UX) - 2H(V|U))\epsilon_2)},
\end{aligned}$$



$$\begin{aligned}
& \mathbb{E}_{C_n}[P_{e_6}] \\
& \leq \sum_{\omega, \nu, k, l} p(\omega, \nu, k, l) \sum_{(x^n, y^n) \in \mathcal{T}_{\epsilon_1}^n(XY)} p(x^n, y^n) \\
& \quad \mathbb{E}_{C_n} \left[ \mathbb{1} \{ \forall \tilde{l}, (x^n, u^n(\omega, \nu), v^n(\omega, \nu, k, \tilde{l})) \notin \mathcal{T}_{\epsilon_2}^n(XUV) \text{ and } (x^n, u^n(\omega, \nu)) \in \mathcal{T}_{\epsilon}^n(XU) \} \right] \\
& \leq \sum_{\omega, \nu, k, l} p(\omega, \nu, k, l) \sum_{(x^n, y^n) \in \mathcal{T}_{\epsilon_1}^n(XY)} p(x^n, y^n) \\
& \quad \left( \mathbb{P} \left[ (x^n, U^n(\omega, \nu), V^n(\omega, \nu, k, \tilde{l})) \notin \mathcal{T}_{\epsilon_2}^n(XUV) \text{ and } (x^n, U^n(\omega, \nu)) \in \mathcal{T}_{\epsilon}^n(XU) \right] \right)^{2^{nR'_v}} \\
& \leq \sum_{\omega, \nu, k, l} p(\omega, \nu, k, l) \sum_{(x^n, y^n) \in \mathcal{T}_{\epsilon_1}^n(XY)} p(x^n, y^n) \\
& \quad \left( \sum_{u^n: (u^n, x^n) \in \mathcal{T}_{\epsilon}^n(UX)} p(u^n) \mathbb{P} \left[ (x^n, u^n(\omega, \nu), V^n(\omega, \nu, k, \tilde{l})) \notin \mathcal{T}_{\epsilon_2}^n(XUV) \right] \right)^{2^{nR'_v}} \\
& \leq \left( \delta_{\epsilon, \epsilon_2}^{(5)} \right)^{2^{nR'_v}},
\end{aligned}$$

where  $\delta_{\epsilon_1, \epsilon}^{(5)} \triangleq 2|\mathcal{X}||\mathcal{U}||\mathcal{V}| \exp \left( -n \frac{(\epsilon_2 - \epsilon)^2}{1 + \epsilon} \mu_{XUV} \right)$ . All in all  $\mathbb{E}_{C_n}[P_e(\epsilon, n, \mathcal{C}_n)]$  goes to zero as  $n\epsilon^2$  goes to infinity, and we conclude with the selection lemma [13].

## APPENDIX G

### COMPLEMENTS FOR THE PROOF OF THEOREM 5

#### A. Reconciliation capacity

Let  $R_1, R_2 \in \mathbb{R}^+$ .

1) *Converse*: We first establish the rate constraints on  $R_1$  and  $R_2$ . We have

$$\begin{aligned}
nR_1 & \geq H(A) \\
& \geq I(A; X^n) \\
& \geq I(A; X^n) - I(A; Y^n) \\
& \stackrel{(a)}{=} n[I(A; X_J | \tilde{U}) - I(A; Y_J | \tilde{U})] \\
& \stackrel{(b)}{=} n[I(U; X_J) - I(U; Y_J)] \\
& \stackrel{(c)}{=} nI(U; X_J | Y_J)
\end{aligned} \tag{44}$$

where (a) holds by [28, Lemma 4.1], if we set  $\tilde{U} = X^{J-1} Y_{J+1}^N J$  and  $J$  is a **RV** uniformly distributed on  $\llbracket 1, n \rrbracket$ , independent of all previous **RVs**, (b) holds if we set  $U = A\tilde{U}$ , since  $X_J$  and  $\tilde{U}$  are independent,

and (c) holds since  $U \rightarrow X_J \rightarrow Y_J$  forms a Markov chain. Similarly, we have

$$\begin{aligned}
 nR_2 &\geq H(B|A) \\
 &\stackrel{(d)}{\geq} H(B|AY^n) + H(S|\hat{S}) - n\delta(\epsilon) \\
 &\stackrel{(e)}{\geq} I(S; B|AY^n) + H(S|ABY^n) - n\delta(\epsilon) \\
 &= H(S|AY^n) - n\delta(\epsilon) \\
 &= H(S|A) - I(S; Y^n|A) - n\delta(\epsilon) \\
 &\stackrel{(f)}{=} I(S; X^n|A) - I(S; Y^n|A) - n\delta(\epsilon) \\
 &\stackrel{(g)}{=} n[I(V; X_J|U) - I(V; Y_J|U)] - n\delta(\epsilon)
 \end{aligned} \tag{45}$$

where (d) holds by Fano's inequality, since for any  $\epsilon > 0$ , there exists a reconciliation protocol such that  $\mathbb{P}(S \neq \hat{S}) \leq \delta(\epsilon)$ ,<sup>23</sup> (e) holds since  $\hat{S} = \eta_b(Y^n, A, B)$ , (f) holds since  $B = f(X^n, A)$ , (g) holds by [28, Lemma 4.1] and if we set  $V = S$ .

We now determine the reconciliation capacity bound.

$$\begin{aligned}
 I(S; X^n) &= \sum_{i=1}^n I(S; X_i | X^{i-1}) \\
 &\stackrel{(a)}{=} \sum_{i=1}^n I(SX^{i-1}; X_i) \\
 &\leq \sum_{i=1}^n I(SX^{i-1}Y_{i+1}^n; X_i) \\
 &= n \sum_{i=1}^n \mathbb{P}(J = i) I(SX^{J-1}Y_{J+1}^n; X_J | J = i) \\
 &= nI(S\tilde{U}; X_J | J) \\
 &\leq nI(VU; X_J),
 \end{aligned} \tag{46}$$

<sup>23</sup> $\delta(\epsilon)$  denotes a function of  $\epsilon$  such that  $\lim_{\epsilon \rightarrow 0} \delta(\epsilon) = 0$ .

where (a) holds because the  $X_i$ 's are i.i.d.. Then,

$$\begin{aligned}
H(S) - H(AB) &= I(S; X^n) + H(S|X^n) - H(A) - H(B|A) \\
&\stackrel{(b)}{\leq} nI(VU; X_J) - H(A) - H(B|A) \\
&\stackrel{(c)}{\leq} n[I(VU; X_J) - I(U; X_J|Y_J) - I(V; X_J|U) + I(V; Y_J|U) + \delta(\epsilon)] \\
&= n[I(U; Y_J) + I(V; Y_J|U) + \delta(\epsilon)],
\end{aligned}$$

where (b) holds by (46) and since  $S = \eta_a(X^n)$ , and (c) holds by (44) and (46).

For a DMS, standard techniques [28] show that  $|\mathcal{U}| \leq |\mathcal{X}|+2$  and  $|\mathcal{V}| \leq |\mathcal{Y}|$ .

### B. Sequential key distillation

1) *Discrete case:* Let  $\epsilon > 0$ . Let  $R_1, R_2 \in \mathbb{R}^+$ . Let  $m, n \in \mathbb{N}$ , and define  $N \triangleq nm$ . Let  $k \in \mathbb{N}$  to be determined later. Consider a sequential key-distillation strategy  $\mathcal{S}_N$  that consists of

- $m$  repetitions of a reconciliation protocol  $\mathcal{R}_n$  based on Wyner-Ziv coding. After one repetition of the protocol, Alice obtains  $S^n = (U^n V^n)$ , whereas Bob has  $\hat{S}^n = (\hat{U}^n \hat{V}^n)$  with  $\mathbb{P}[\hat{U}^n \neq U^n] \leq \delta_\epsilon(n)$ ,<sup>24</sup>  $\mathbb{P}[\hat{V}^n \neq V^n] \leq \delta_\epsilon(n)$ ,  $\mathbb{P}[\hat{S}^n \neq S^n] \leq P_e(\epsilon, n)$ <sup>25</sup> and  $(U^n, V^n, X^n)$ ,  $(\hat{U}^n, \hat{V}^n, Y^n)$ , jointly typical with probability approaching one for  $n$  large. In addition, the information disclosed over the public channel during the  $m$  repetition of the reconciliation protocol is upper bounded by  $\log|\mathcal{A}|^N + \log|\mathcal{B}|^N = NI(U; X|Y) + NI(V; X|YU) + Nr_0(\epsilon)$ , with  $\lim_{\epsilon \rightarrow 0} r_0(\epsilon) = 0$ ;
- privacy amplification based on extractors, with output size  $k$ , at the end of which Alice computes her key  $K = g(S^m, U_d)$ , while Bob computes  $\hat{K} = g(\hat{S}^m, U_d)$ , where  $U_d$  is a sequence of  $d$  uniformly distributed random bits.

The total information available to Eve after reconciliation consists of her observation  $Z^N$ , the public messages  $A^N$  and  $B^N$  sent by Alice, and  $U_d$ . The strategy  $\mathcal{S}_N$  is also known to Eve, but we omit the conditioning on  $\mathcal{S}_N$  for convenience.

<sup>24</sup> $\delta_\epsilon(n)$  denotes a function of  $\epsilon$  and  $n$  such that  $\lim_{n \rightarrow \infty} \delta_\epsilon(n) = 0$ .

<sup>25</sup>We can show that  $P_e(\epsilon, n)$  decreases exponentially to zero as  $n\epsilon^2$  goes to infinity.

We first show that, for a suitable choice of the output size  $k$ , we have  $k \geq H(K|U_d Z^N A^N B^N) \geq k - \delta(N)$ .<sup>26</sup> Let us start by defining the following RVs

$$\Theta \triangleq \begin{cases} 1 & \text{if } (S^N, Z^N) \in \mathcal{T}_{2\epsilon}^m(S^n Z^n) \text{ and } Z^N \in \mathcal{T}_\epsilon^m(Z^n), \\ 0 & \text{otherwise.} \end{cases}$$

$$\Upsilon \triangleq \begin{cases} 1 & \text{if } H_\infty(S^N|z^N, a^N, b^N, \Theta = 1) \leq \log(|\mathcal{A}|^N |\mathcal{B}|^N) + \sqrt{N}, \\ 0 & \text{otherwise.} \end{cases}$$

By Lemma 2 applied to the DMS  $(\mathcal{U}^n \mathcal{V}^n Z^n, p_{S^n Z^n})$ ,  $\mathbb{P}(\Theta = 1) \geq 1 - \delta_\epsilon^0(m)$ , and by [9, Lemma 10],  $\mathbb{P}(\Upsilon = 1) \geq 1 - 2^{-\sqrt{N}}$ . Hence,  $\mathbb{P}(\Upsilon = 1, \Theta = 1) \geq 1 - \delta_\epsilon^0(m) - 2^{-\sqrt{N}}$ , and

$$H(K|U_d Z^N A^N B^N) \geq (1 - \delta_\epsilon^0(m) - 2^{-\sqrt{N}}) H(K|U_d Z^N A^N B^N, \Upsilon = 1, \Theta = 1). \quad (47)$$

To lower bound  $H(K|U_d Z^N A^N B^N, \Upsilon = 1, \Theta = 1)$ , we first lower bound  $H_\infty(S^N|Z^N = z^N, A^N = a^N, B^N = b^N, \Theta = 1, \Upsilon = 1)$  to be able to use Theorem 3. By definition of  $\Upsilon$ ,

$$\begin{aligned} & H_\infty(S^N|Z^N = z^N, A^N = a^N, B^N = b^N, \Theta = 1, \Upsilon = 1) \\ & \geq H_\infty(S^N|Z^N = z^N, \Theta = 1) - \log(|\mathcal{A}|^N |\mathcal{B}|^N) - \sqrt{N} \\ & \stackrel{(a)}{\geq} m(H(S^n|Z^n) - \delta(\epsilon)) - \delta_\epsilon^1(m) - N(I(U; X|Y) + I(V; X|YU)) - \sqrt{N} - Nr_0(\epsilon), \end{aligned} \quad (48)$$

where (a) follows from Lemma 2, and  $\log(|\mathcal{A}|^N |\mathcal{B}|^N) = N(I(U; X|Y) + I(V; X|YU)) + Nr_0(\epsilon)$ . We now lower bound  $H(S^n|Z^n)$ . We first remark that

$$\begin{aligned} H(S^n|Z^n) &= I(X^n; S^n|Z^n) + H(S^n|X^n Z^n) \\ &= H(X^n|Z^n) - H(X^n|Z^n S^n) + H(U^n|X^n Z^n) + H(V^n|X^n U^n Z^n) \\ &\stackrel{(b)}{=} nH(X|Z) - H(X^n|Z^n S^n), \end{aligned} \quad (49)$$

where (b) holds since  $U^n$  and  $V^n$  are functions of  $X^n$ , and because the  $Y_i$ 's and  $Z_i$ 's are i.i.d..

We lower bound the term  $-H(X^n|Z^n S^n)$  in (49). Define

$$\Gamma_1 \triangleq \begin{cases} 1 & \text{if } (X^n U^n, V^n, Z^n) \in T_{2\epsilon}^n((XU)VZ), \\ 0 & \text{otherwise.} \end{cases}$$

$$\Delta_1 \triangleq \begin{cases} 1 & \text{if } (X^n U^n, V^n) \in T_\epsilon^n((XU)V), \\ 0 & \text{otherwise.} \end{cases}$$

<sup>26</sup> $\delta(n)$  denotes a function of  $n$  such that  $\lim_{n \rightarrow \infty} \delta(n) = 0$ .

We can write

$$\begin{aligned}
H(X^n|Z^n S^n) &\leq H(X^n \Gamma_1 \Delta_1 | Z^n S^n) \\
&= H(\Gamma_1 \Delta_1 | Z^n S^n) + H(X^n | Z^n S^n \Gamma_1 \Delta_1) \\
&\leq 2 + \sum_{\delta_1, \gamma_1 \in \{0,1\}} \mathbb{P}(\Gamma_1 = \gamma_1 | \Delta_1 = \delta_1) \mathbb{P}(\Delta_1 = \delta_1) H(X^n | Z^n S^n, \Gamma_1 = \gamma_1, \Delta_1 = \delta_1) \\
&\stackrel{(c)}{\leq} 2 + H(X^n | Z^n S^n, \Gamma_1 = 1, \Delta_1 = 1) + n(2\delta_\epsilon^2(n) + \delta_\epsilon^3(n)/2) \log|\mathcal{X}|,
\end{aligned} \tag{50}$$

where (c) holds since  $\mathbb{P}(\Delta_1 = 0) \leq \delta_\epsilon^2(n)$ ,<sup>27</sup> and  $\mathbb{P}(\Gamma_1 = 0 | \Delta_1 = 1) \leq \delta_\epsilon^3(n)/2$ .<sup>28</sup> Indeed, we can apply Markov Lemma (see the version in [31]), since we have  $V^n \rightarrow X^n U^n \rightarrow Z^n$  and for every  $((xu)^n, z^n)$ ,  $p(z^n | x^n u^n) = p(z^n | x^n) = \prod_{i=1}^n p_{Z|X}(z_i | x_i) = \prod_{i=1}^n p_{Z|XU}(z_i | x_i u_i)$ , because  $U^n \rightarrow X^n \rightarrow Z^n$ . Then,

$$\begin{aligned}
&H(X^n | Z^n S^n, \Gamma_1 = 1, \Delta_1 = 1) \\
&= \sum_{z^n, s^n} p(z^n, s^n | 1, 1) H(X^n | Z^n = z^n, S^n = s^n, \Gamma_1 = 1, \Delta_1 = 1) \\
&\leq \sum_{z^n, s^n} p(z^n, s^n | 1, 1) \log |T_{2\epsilon}^n(X | z^n, s^n)| \\
&\leq \sum_{z^n, s^n} p(z^n, s^n | 1, 1) (nH(X|ZS)(1 + 2\epsilon)) \\
&\leq nH(X|ZS)(1 + 2\epsilon).
\end{aligned} \tag{51}$$

Hence by (50), (51),

$$H(X^n | Z^n S^n) \leq nH(X|ZS) + r_2(\epsilon, n), \tag{52}$$

where

$$r_2(\epsilon, n) \triangleq 2nH(X|ZS)\epsilon + n(2\delta_\epsilon^2(n) + \delta_\epsilon^3(n)/2) \log|\mathcal{X}| + 2. \tag{53}$$

Combining (49), (52),

$$H(S^n | Z^n) \geq n[H(X|Z) - H(X|ZS)] - r_2(\epsilon, n). \tag{54}$$

<sup>27</sup>We have  $\delta_\epsilon^2(n) \leq P_e(\epsilon, n)$  by Wyner-Ziv coding in the reconciliation protocols.

<sup>28</sup>By Markov Lemma, we have  $\delta_\epsilon^3(n) \triangleq 2|S_{XUZ}|e^{-\epsilon^2 n \mu_{XUZ}/6}$ .

Then, remark that

$$\begin{aligned}
& H(X|Z) - H(X|ZS) \\
&= I(X; S|Z) \\
&= H(U|Z) + H(V|UZ) - H(U|XZ) - H(V|UXZ) \\
&\stackrel{(d)}{\geq} H(U|Z) + H(V|UZ) - H(U|X) - H(V|UX) \\
&= I(U; X) - I(U; Z) - I(V; Z|U) + I(V; X|U),
\end{aligned} \tag{55}$$

where (d) holds because conditioning reduces entropy. Hence, by (48), (54) and (55)

$$\begin{aligned}
& H_\infty(S^N|Z^N = z^N, A^N = a^N, B^N = b^N, \Theta = 1, \Upsilon = 1) \\
&\geq N[I(U; Y) + I(V; Y|U) - I(U; Z) - I(V; Z|U)] - r_3(\epsilon, N),
\end{aligned} \tag{56}$$

where

$$r_3(\epsilon, N) \triangleq m(r_2(\epsilon, n) + \delta(\epsilon)) + \delta_\epsilon^1(m) + Nr_0(\epsilon) + \sqrt{N}. \tag{57}$$

Set  $k$  to be less than the lower bound in (56) by  $\sqrt{N}$ :

$$k \triangleq \lfloor N[I(U; Y) + I(V; X|U) - I(U; Z) - I(V; Z|U)] - r_3(\epsilon, N) - \sqrt{N} \rfloor. \tag{58}$$

Now that we have lower bounded  $H_\infty(S^N|Z^N = z^N, A^N = a^N, B^N = b^N, \Theta = 1, \Upsilon = 1)$  in (56) by  $k$  (defined in (58)), we can apply Theorem 3 to lower bound  $H(K|U_d Z^N A^N B^N, \Upsilon = 1, \Theta = 1)$  by  $k - N\delta^*(N)$ , where  $\delta^*(N)$  is defined in the theorem. Thus, we can finally lower bound  $H(K|U_d Z^N A^N B^N)$  in (47):

$$H(K|U_d Z^N A^N B^N) \geq \left(1 - \delta_\epsilon^0(m) - 2^{-\sqrt{N}}\right) (k - N\delta^*(N)) = k - \delta(N),$$

where the equality is obtained thanks to the exponential decrease of  $\delta^*$  and  $\delta_\epsilon^0$ . Moreover, the leakage is such that

$$I(K; U_d Z^N A^N B^N) = H(K) - H(K|U_d Z^N A^N B^N) \leq \delta(N). \tag{59}$$

The keys computed by Alice and Bob are almost the same as  $N$  goes to infinity, since

$$\mathbb{P}(K \neq \hat{K}) \leq \mathbb{P}(S^N \neq \hat{S}^N) \leq m\mathbb{P}((U^n V^n) \neq (\hat{U}^n \hat{V}^n)) \leq mP_e(\epsilon, n), \tag{60}$$

Then, by (53), (57), we have that  $r_3(\epsilon, N)/N = \delta(N) + \delta(\epsilon)$ , thus the secret key rate  $R \triangleq k/N$  is

$$R = I(U; Y) - I(U; Z) + I(V; Y|U) - I(V; Z|U) - \delta(\epsilon) - \delta(N).$$

We finish the proof as follows. If  $I(V; Y|U) \leq I(V; Z|U)$ , in the reconciliation we set  $R_2 = 0$  so that we now have

$$R = I(U; Y) - I(U; Z) + [I(V; Y|U) - I(V; Z|U)]^+ - \delta(\epsilon) - \delta(N).$$

Then, if  $I(U; Y) \leq I(U; Z)$ , in the reconciliation protocol, we choose  $S = V$  (see the beginning of the proof), and we assume that  $U^N$  is provided by a genie to Eve. Consequently, we obtain instead of Equation (48),

$$\begin{aligned} H_\infty(V^N | Z^N = z^N, U^N = u^N, B = b, \Theta = 1, \Upsilon = 1) \\ \geq m(H(V^n | Z^n U^n) - \delta(\epsilon)) - \delta_\epsilon^1(m) - NI(V; X|YU) - \sqrt{N} - Nr_0(\epsilon), \end{aligned}$$

and conclude in the same manner, to obtain

$$R = [I(U; Y) - I(U; Z)]^+ + [I(V; Y|U) - I(V; Z|U)]^+ - \delta(\epsilon) - \delta(N).$$

2) *Continuous case:* We proceed as in the proof of Theorem 4 in Appendix B-A2.

## REFERENCES

- [1] U. M. Maurer, “Secret Key Agreement by Public Discussion from Common Information,” *IEEE Trans. Inf. Theory*, vol. 39, pp. 733–742, 1993.
- [2] R. Ahlswede and I. Csiszár, “Common Randomness in Information Theory and Cryptography Part I: Secret Sharing,” *IEEE Trans. Inf. Theory*, vol. 39, pp. 1121–1132, 1993.
- [3] I. Csiszár and P. Narayan, “Common Randomness and Secret Key Generation with a Helper,” *IEEE Trans. Inf. Theory*, vol. 46(2), pp. 344–366, 2000.
- [4] F. Grosshans, G. V. Assche, J. Wenger, R. Brouri, N. Cerf, and P. Grangier, “Quantum Key Distribution using Gaussian-Modulated Coherent States,” *Nature*, vol. 421, pp. 238–241, 2003.
- [5] G. V. Assche, J. Cardinal, and N. J. Cerf, “Reconciliation of a Quantum-Distributed Gaussian Key,” *IEEE Trans. Inf. Theory*, vol. 50, no. 2, pp. 394–400, 2004.
- [6] M. Bloch, J. Barros, M. Rodrigues, and S. McLaughlin, “Wireless Information-Theoretic Security,” *IEEE Trans. Inf. Theory*, vol. 54(6), pp. 2515–2534, 2008.
- [7] G. Brassard and L. Salvail, “Secret-Key Reconciliation by Public Discussion.” Springer-Verlag, 1994, pp. 410–423.
- [8] C. Bennett, G. Brassard, and U. Maurer, “Generalized Privacy Amplification,” *IEEE Trans. Inf. Theory*, vol. 41, pp. 1915–1923, 1995.
- [9] U. Maurer and S. Wolf, “Information-Theoretic Key Agreement: From Weak to Strong Secrecy for Free,” in *Lecture Notes in Computer Science*. Springer-Verlag, 2000, pp. 351–368.
- [10] I. Csiszár and P. Narayan, “Secrecy Capacities for Multiple Terminals,” *IEEE Trans. Inf. Theory*, vol. 50(12), pp. 3047–3061, 2004.
- [11] M. Bloch, A. Thangaraj, S. McLaughlin, and J.-M. Merolla, “LDPC-Based Gaussian Key Reconciliation,” in *IEEE Inf. Theory Workshop*, 2006.

- [12] D. Elkouss, A. Leverrier, R. Alleaume, and J. Boutros, “Efficient Reconciliation Protocol for Discrete-Variable Quantum Key Distribution,” *IEEE Int. Symp. Inf. Theory*, pp. 1879–1883, 2009.
- [13] M. Bloch and J. Barros, *Physical-Layer Security: from Information Theory to Security Engineering*. Cambridge University Press, 2011.
- [14] S. Nitinawarat and P. Narayan, “Secret Key Generation for Correlated Gaussian Sources,” *IEEE Trans. Inf. Theory*, vol. 58, no. 6, pp. 3373–3391, 2012.
- [15] R. Chou and M. Bloch, “One-Way Rate-Limited Sequential Key-Distillation,” in *IEEE Int. Symp. Inf. Theory*, 2012.
- [16] S. Watanabe and Y. Oohama, “Secret Key Agreement from Correlated Gaussian Sources by Rate Limited Public Communication,” *IEICE Trans. Fundamentals*, vol. E93A, 2010.
- [17] S. Vadhan, “Extracting All the Randomness from a Weakly Random Source,” Electronic Colloquium on Computational Complexity, Tech. Rep., 1998.
- [18] M. V. Dijk, “On a Special Class of Broadcast Channels with Confidential Messages,” *IEEE Trans. Inf. Theory*, vol. 43, no. 2, pp. 712–714, 1997.
- [19] M. Dür, R. Horst, and M. Locatelli, “Necessary and Sufficient Global Optimality Conditions for Convex Maximization Revisited,” *Journal of Mathematical Analysis and Applications*, vol. 217, pp. 637–649, 1998.
- [20] R. Gallager, *Information Theory and Reliable Communication*. John Wiley and Sons, New York, 1968.
- [21] Y. Yang, S. Cheng, Z. Xiong, and W. Zhao, “Wyner-Ziv Coding Based on TCQ and LDPC Codes,” *IEEE Trans. Commun.*, vol. 57, no. 2, 2009.
- [22] D. Elkouss, J. Martinez, D. Lancho, and V. Martin, “Rate Compatible Protocol for Information Reconciliation: An Application to QKD,” *IEEE Inf. Theory Workshop*, pp. 145–149, 2010.
- [23] K. Kasai, R. Matsumoto, and K. Sakaniwa, “Information Reconciliation for QKD with Rate-Compatible Non-Binary LDPC Codes,” in *ISITA’10*, 2010, pp. 922–927.
- [24] L. Carter and M. Wegman, “Universal Classes of Hash Functions,” *Journal of Computer and System Sciences*, vol. 18, no. 2, pp. 143–154, 1979.
- [25] R. Rockafellar, *Convex Analysis*. Princeton University Press, Princeton, NJ, 2011.
- [26] D. Oates, “A Non-Compact Krein-Milman Theorem,” *Pacific Journal of Mathematics*, vol. 36, 1971.
- [27] M. Kashimoto and M. Nashed, “A Note on Factorization of Bounded Linear Operators,” *Communications in Applied Analysis*, vol. 10, 2006.
- [28] R. Ahlswede and I. Csiszár, “Common Randomness in Information Theory and Cryptography Part II: CR Capacity,” *IEEE Trans. Inf. Theory*, vol. 44, pp. 225–240, 1998.
- [29] A. Wyner and J. Ziv, “The Rate Distortion Function for Source Coding with Side Information at the Decoder,” *IEEE Trans. Inf. Theory*, vol. 22(1), pp. 1–10, 1973.
- [30] G. Kramer, “Topics in Multi-User Information Theory,” *Foundations and Trends in Communications and Information Theory*, vol. 4, pp. 265–444, 2007.
- [31] A. Orlitsky and J. Roche, “Coding for Computing,” *IEEE Trans. Inf. Theory*, vol. 47, no. 3, 2001.
- [32] T. Berger, *Multiterminal Source Coding*. The Information Theory Approach to Communications, G.Longo, Ed. New York: Springer-Verlag, 1978.
- [33] R. M. Fano, *Transmission of Information: A Statistical Theory of Communications*. M.I.T. Press, 1961.
- [34] M. S. Pinsker, *Information and Information Stability of Random Variables and Processes*. Holden-Day, 1964.
- [35] T. Cover and J. Thomas, *Elements of Information Theory*. Wiley, 1991.



- [36] M. Salehi, “Cardinality Bounds on Auxiliary Variables in Multiple-User Theory via the Method of Ahlswede and Körner,” Electronic Colloquium on Computational Complexity, Tech. Rep., 1998.
- [37] A. E. Gamal and Y.-H. Kim, *Network Information Theory*. Cambridge University Press, 2011.